SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA ANGLISTIKU
SMJER: PREVODITELJSKI
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
SMJER: ARHIVISTIKA
Ak. god. 2018/19.

Andro Babić

Prevođenje terminologije ulančanih blokova

Interdisciplinarni diplomski rad

Mentori: dr. sc. Nataša Pavlović, izv. prof.
dr. sc. Hrvoje Stančić, red. prof.

Zagreb, rujan 2019.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____
(potpis)

Zahvala

Ovim putem zahvaljujem se, srdačno i iskreno, svojim mentorima dr. sc. Nataši Pavlović i dr. sc. Hrvoju Stančiću, koji su mi svojom ekspertizom, iskustvom i strpljenjem olakšali pisanje ovog diplomskog rada, nadalje zahvaljujem se svojoj obitelji i najbližima na bezuvjetnoj podršci, kao i prijateljima i kolegama koji su mi studentske dane ispunili vedrinom.

SAŽETAK
Prevođenje terminologije ulančanih blokova

Tema ovog diplomskog rada je terminologija blockchain tehnologije. Blockchain, ili ulančani blokovi recentna su tehnologija za koju se pokazao izniman interes na svjetskim tržištima. Korištenje takve disruptivne tehnologije unutar jezične skupine zahtjeva razumijevanje problematike na jeziku te skupine. U ovom slučaju riječ je o hrvatskom jeziku koji se izrazito polagano prilagođava tehnološkim inovacijama. Činjenica da tehnologija ulančanih blokova ima niz potencijalnih primjena u raznim aspektima poslovanja i ljudskog života ukazuje na potrebu za popisivanjem ujednačavanjem i opisivanjem terminologije te tehnologije. Rad je interdisciplinaran: iz perspektive arhivistike sagledava tehnologiju koja je usko povezana s čuvanjem zapisa, dok iz perspektive terminologije i terminografije promatra engleske termine te njihove potencijalne terminološke ekvivalente na hrvatskome jeziku. Istraživanjem provedenim u sklopu rada ispituju se stavovi struke o ponuđenim terminima na hrvatskom jeziku. Rad je stoga zamišljen kao primjer dobre jezične prakse obrađivanja terminologije disruptivnih tehnologija. Ispitivanje stavova struke o novim terminima koji se javljaju pojavom tehnologije ulančanih blokova jedna je od aktivnosti kojima se struka uključuje u popisivanje termina, što ovom radu daje dodanu znanstvenu i stručnu vrijednost. Na temelju rezultata istraživanja, krajnji je cilj ponuditi prijevode termina koje će prihvatiti struka i javnost te omogućiti pristup terminološkoj bazi putem Interneta.

Ključne riječi: terminologija, terminografija, arhivistika, ulančani blokovi, blockchain, distribuirana glavna knjiga, DLT, bitcoin

SUMMARY
Translating blockchain terminology

The topic of this master's thesis is the terminology of blockchain technology. Blockchain is a recent technology which has sparked great interest on markets around the globe. Reaping the benefits from this disruptive technology within a language community requires complete understanding of the topic in the language of the community, particularly in cases when a language tends to be rather slow to adapt to technological innovation, such as Croatian. The fact that blockchain technology has numerous potential uses which can improve different business activities and daily life suggests that it is important to catalogue, unify and describe the terminology. The paper is interdisciplinary: from the perspective of archival studies, it deals with a technology closely related to recordkeeping and digital preservation, whereas from the perspective of terminology and terminography, it deals with English terms used to describe the technology and with their potential Croatian terminological equivalents. The research carried out as part of the master's thesis investigates the attitudes of professionals with regard to Croatian term candidates related to blockchain technology. This paper is therefore envisaged as an example of best practice in working with the terminology of disruptive technologies. By investigating the attitudes of professionals with regard to new terms which have emerged with the blockchain technology, professionals are involved in the process of terminography, which gives this master's thesis added value. Based on the research results, the aim is to propose Croatian terms which are expected to be adopted by professionals and the general public, as well as to make the data accessible by sharing the termbase online.

Keywords: terminology, terminography, archival science, blockchain, distributed ledger, DLT, bitcoin

SADRŽAJ

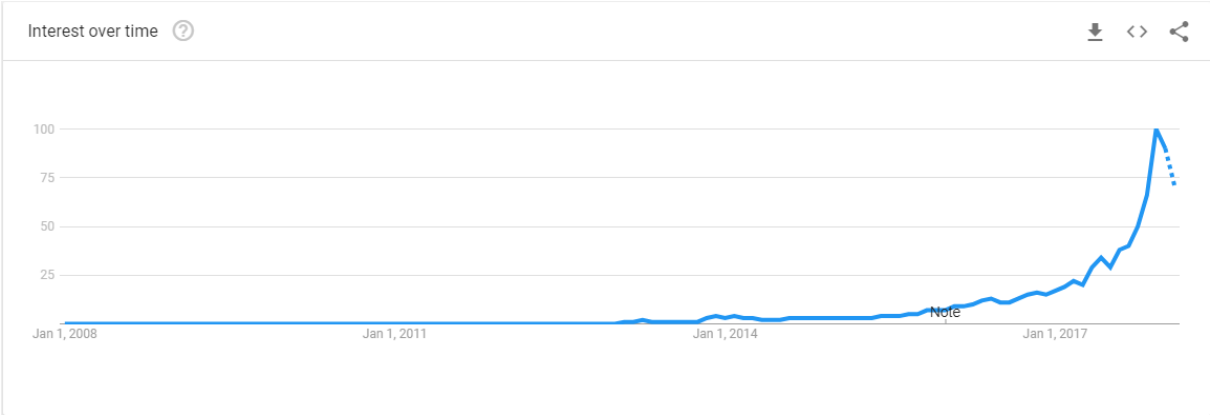
1. UVOD

Blockchain ili tehnologija ulančanih blokova je recentna, ometajuća ili disruptivna tehnologija čiji je hitri razvoj i strmoglavi rast popularnosti nadmašio mogućnosti znanstvene zajednice da opiše i definira tu računalnu tehnologiju i sve njezine funkcije. Trend institucionalne nezainteresiranosti naglo se promijenio proteklih godina kada su razni oblici odgovorne i ekonomski isplative uporabe tehnologije ulančanih blokova razbili stigmu sive ekonomije i nelegalnog trgovanja novcem. Literatura koja se bavi ovom tematikom obiluje konfliktnim definicijama i shvaćanjima ključnih pojmova te će se u ovom radu pokušati ponuditi različite interpretacije kako bi stvorio što cjelovitiju sliku tehnologije ulančanih blokova, njene povijesti, potencijalne primjene i tehničkih funkcionalnosti u svrhu popisivanja i prevođenja terminologije vezane uz nju.

Prva, i do danas najuspješnija primjena tehnologije ulančanih blokova zasigurno je digitalna valuta bitcoin. U bijeloj knjizi bitcoina iz 2008. godine naslovljenom „*Bitcoin: A Peer-to-Peer Electronic Cash System*“ prvi je puta predloženo korištenje ulančanih blokova kao temelja za sustav digitalnog plaćanja.[1] Članak potpisuje Satoshi Nakamoto, što je pseudonim za autora ili autore zadužene za osmišljanje i implementaciju prvog sustava ulančanih blokova, a do danas nije otkriveno tko stoji iza tog pseudonima..[2] Bitcoin se još naziva i kriptovalutom (eng. *cryptocurrency*), jer je cijela tehnologija utemeljena na kriptografiji. Od 2008. bitcoin bilježi nagli rast u vrijednosti, a platforma doživljava stostruki porast korisnika. Po uzoru na bitcoin nastaju alternativne kriptovalute (eng. *altcoin*), od kojih se kao najuspješnija pokazala kriptovaluta Ethereum. Uspjeh implementacije tehnologije ulančanih blokova u projekt bitcoin otvorio je vrata novim interpretacijama i primjenama ove tehnologije. Alternativne kriptovalute najbolji su pokazatelj svestranosti tehnologije i njenih šarolikih primjena. Osim kriptovaluta, tržišni uspjeh doživjele su i platforme za razvoj *blockchaina* u poslovanju. Hyperledger, projekt Linux Foundationa nudi alate otvorenog koda za razvoj sustava ulančanih blokova i aplikacija na njima, dok IBM Blockchain platforma nudi komercijalna rješenja te usluge razvoja i implementacije ulančanih blokova u poslovanje i komunikaciju između institucija.[3, 4]

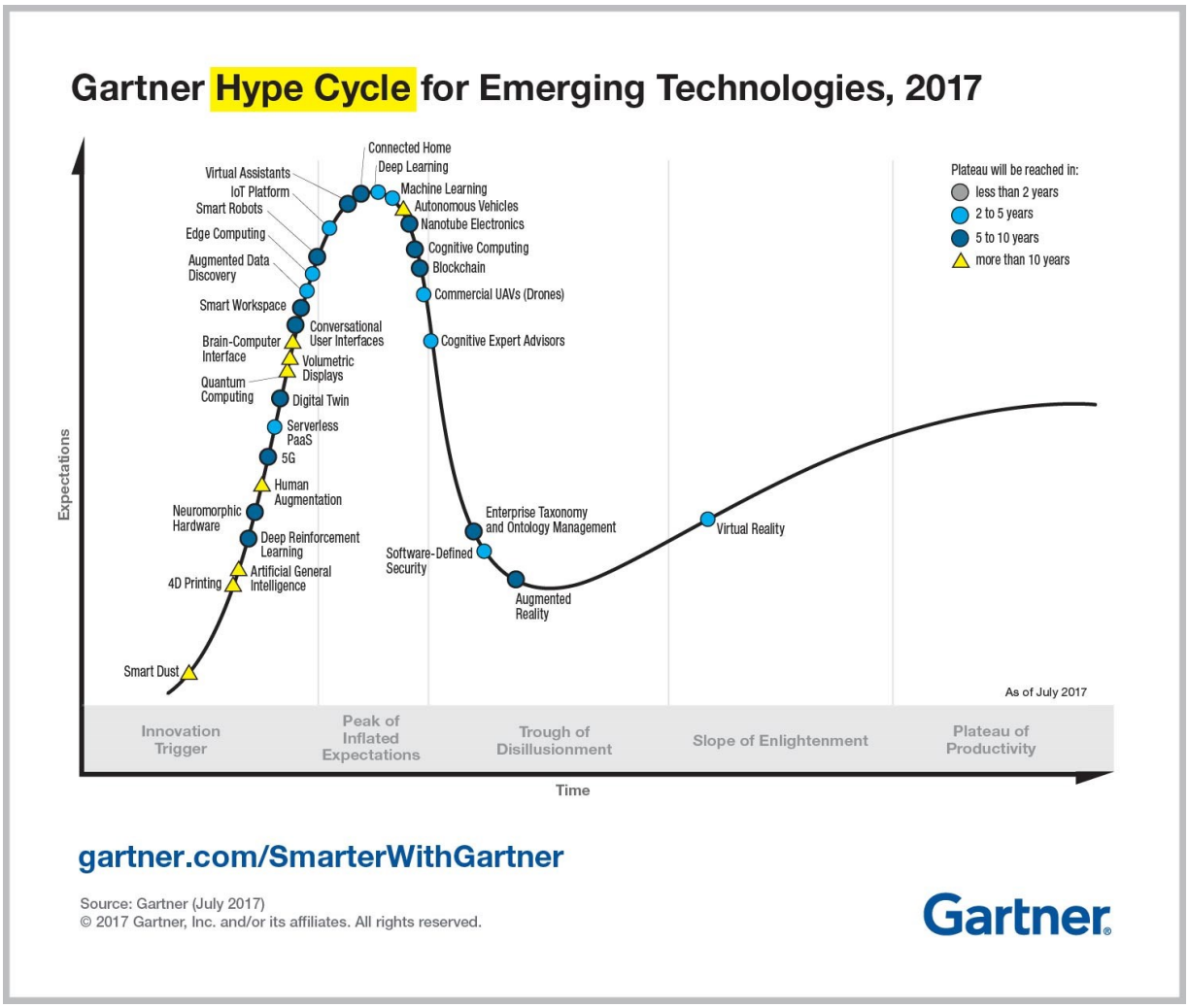
[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (2008.), 1. URL: https://bitcoin.org/bitcoin.pdf
[2] Zoe Bernard, Everything you need to know about Bitcoin, (Business Insider, 2018.) URL: http://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12/#but-satoshi-nakamoto-didnt-work-entirely-alone-3
[3] Hyperledger, About Hyperledger (Linux Foundation, 2018.) URL: https://www.hyperledger.org/about

Popularnost ove tehnologije najbolje se može prikazati upravo iz mrežnih izvora. Usluga Google trendovi dobar je pokazatelj interesa javnosti za temu, jer bilježi broj pretraživanja određenog pojma kroz vrijeme. Tehnologija je svijetu predstavljena 2008. godine te od sredine 2013. godine interes za nju blago raste, a od početka 2016. bilježi drastičan porast javnog interesa (Grafikon 1). U svrhu mjerenja ciklusa trendova u informacijskim tehnologijama tvrtka Gartner razvila je *hype cycle*, vizualni prikaz razvoja tehnoloških trendova koji počinju inovacijom, nakon čega trendovi prolaze kroz vrhunac preuveličanih očekivanja, nakon kojeg slijedi pad uzrokovan razočaranjem u tehnologiju te se tek uslijed razočaranja postiže razumijevanje ili prosvjetljenje, nakon kojeg slijedi plato produktivnosti u kojem tehnologija zaista doživljava svoj potpuni potencijal. Prema metodologiji tvrtke Gartner, ulančani blokovi vrhunac će funkcionalnosti doživjeti tek za pet do deset godina, a trenutno se nalaze na prijelazu iz faze preuveličanih očekivanja u fazu razočaranja (Grafikon 2). Ulančani blokovi u ciklusu trendova prate sličnu putanju kao i slijedeće napredne tehnologije: autonomna vozila, pametni domovi i strojno učenje. Razumijevanje ciklusa trendova važno je kako bi se izbjeglo preuveličavanje važnosti neke tehnologije. Senzacionalizam, tehnološki entuzijazam i optimizam utječu na pogrešno tumačenje i razumijevanje ometajućih tehnologija. Naime, prepoznavanje potencijala neke tehnologije da promijeni svijet, i realizacija te promjene dva su događaja često udaljena desecima godina. *Hype cycle* tvrtke Gartner ukazuje na dvije ključne činjenice o tehnologiji ulančanih blokova, ona je trenutno izrazito popularna i atraktivna ulagačima, znanstvenicima i javnosti, no i dalje je tehnologija u povojima čiji rastući trend nipošto ne jamči potpunu realizaciju svih pretpostavljenih promjena. Istraživanju i interpretaciji tehnologije stoga treba pristupiti s dozom skepse.



Grafikon 1. - Google trends, popularnost pretraživanja pojma „blockchain“

[4] IBM, IBM Blockchain platform (IBM, 2018.) URL: https://www.ibm.com/blockchain/platform/



Grafikon 2. - Gartnerov ciklus trendova

Jedan od alata kojim se može potaknuti i olakšati istraživanje novih tehnoloških trendova unutar jedne jezične zajednice zasigurno je uspostava terminologije. Riječima Dirka Geeraertsa terminologija je „leksička komponenta specijaliziranog jezika koja se javlja iz teorijskih i tehnoloških inovacija, novih znanstvenih uvida i novih alata koji obogaćuju konceptualna i praktična okruženja stručnjaka i u tom procesu šire njihove vokabulare.“[5] Iz prethodnih paragrafa jasno je pokazano da su ulančani blokovi upravo takva tehnologija. Problem nastaje u prenošenju terminologije iz engleskog u hrvatski jezik, naime računalna tehnologija razvija se na engleskom jeziku u kojem se terminologija razvija prirodno uz tehnologiju. Na hrvatskom jeziku spontani razvoj terminologije trajao bi predugo. Potreba za razvojem i standardizacijom terminologije na hrvatskom jeziku jasno je vidljiva jer je tema ulančanih blokova sve više prisutna u sferi javnog života, medija, poslovanja i znanstvenog

[5] Hendrik J. Kockaert, Frieda Steurs-Handbook of Terminology Volume 1 (John Benjamins Publishing Company, 2015), 18.

istraživanja. Tu potrebu prepoznale su i druge skupine, poput Međunarodnog ureda za standarde, čiji se rad na terminologiji ulančanih blokova odvija usporedno s ovim sakupljanjem i istraživanjem terminologije ulančanih blokova.[6,7] Budući da Međunarodni ured za standarde posjeduje veće resurse i tim stručnjaka, njihov rad, kada postane dostupan, svakako treba konzultirati u slučaju manjkavosti i nedostataka ovog diplomskog rada.

Izgradnja i razvoj terminologije zahtjevan je proces koji iziskuje prepoznavanje novih pojmova (koncepata), definiranje tih pojmova te iznalaženje odgovarajućih termina za te pojmove. Sagledajmo definicije termina ulančanih blokova iz nedavno objavljene literature. Jacob William u knjizi naslovljenoj „Ulančani blokovi: jednostavni vodič za sve što trebate znati“ ulančane blokove definira kao „skupinu transakcija, koje čine zajedničku glavnu knjigu, koje su upisane u bazu podataka i provjerene od strane više izvora.“[8] Tapscott i Tapscott, iz financijske perspektive, ulančane blokove smatraju „globalnom distribuiranom glavnom knjigom [...] koja omogućuje izravno slanje novca među korisnicima zaobilazeći banke, tvrtke koje izdaju kreditne kartice ili Paypal.“[9] Narayan, Bonneau, Felten, Miller i Goldfeder sa sveučilišta Princeton ulančane blokove opisuju kao „ključnu komponentu bitcoina; glavnu knjigu u koju su na siguran način zapisane sve bitcoin transakcije.“[10] U knjizi „Savladavanje ulančanih blokova“ Imran Bashir ulančane blokove interpretira slijedećim riječima: „Ulančani blokovi u srži su distribuirana glavna knjiga na peer-to-peer mreži, koja je kriptografski osigurana, na koju se mogu isključivo dodavati podaci, koja je nepromjenjiva i koja se može ažurirati isključivo pomoću konsenzusa ili slaganja između ravnopravnih računala na mreži.“[11] Iz definicija jasno se može zaključiti da ulančani blokovi čuvaju zapise, u kontekstu kriptovalute bitcoin čuvaju se zapisi o novčanim transakcijama, no ulančani blokovi kao tehnologija imaju daleko širu primjenu od bilježenja isključivo novčanih transakcija. Nijedna od navedenih definicija nije potpuna, no svaka sadrži relevantan element u definiranju termina ulančani blokovi. Potpunu definiciju nije moguće ponuditi bez detaljnijeg pregleda teme koji će popisati sve tehničke i tehnološke elemente sustava.

---

[6] HZN/TO 307, Ulančani blokovi i tehnologija elektroničke distribuirane glavne knjige, (Hrvatski zavod za norme, 2019.) URL: https://www.hzn.hr/

[7] International Standards Office, ISO/TC 307, Blockchain and electronic distributed ledger technologies, (ISO, 2019.) URL: https://www.iso.org/committee/6266604.html

[8] Jacob William, Blockchain: The Simple Guide To Everythng You need to Know, (Amazon, 2016)

[9] Alex Tapscott, John Tapscott, Blockchain Revolution (Portfolio, 2016.), 45

[10] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfede, Bitcoin and Cryptocurrency Technologies (Princeton University Press, 2016.), 15

[11] Imran Bashir, Deepr insights into decentralization, cryptography, Bitcoin and popular Blockchain frameworks, (Packt, 2017),

1.1. POZICIONIRANJE TEME

Ovaj diplomski rad bavi se popisivanjem i istraživanjem terminologije ulančanih blokova. Osim poznavanja terminografske metodologije, kvalitetan terminološki rad zahtijeva stručnost terminologa u području s kojim se bavi. Theresa M. Cabré, jedna od najvažnijih suvremenih autorica u polju terminologije, smatra da su za kvalitetan terminološki rad potrebna slijedeća znanja: „Ekspertiza u terminologiji: teorija, metodologija i praktično iskustvo, ekspertiza u tematskom području (tipično ju posjeduju stručnjaci za to polje) te ekspertiza u jeziku ili jezicima“.[12] Ovaj rad je stoga strukturiran kako bi zadovoljio sve zahtjeve kvalitetne terminografske prakse. Koristeći znanja dvaju ekspertnih polja – informacijskih i komunikacijskih znanosti te anglistike kao i savjet stručnjaka i podatke prikupljene u istraživanju jezika, rad će pokušati razjasniti terminologiju recentne tehnologije te ponuditi suvisle terminološke ekvivalente na hrvatskom jeziku, u nadi da će time olakšati ovladavanje tehnologijom korisnicima unutar hrvatske jezične zajednice.

Motivacija za ovu temu proizlazi iz prepoznavanja jezične potrebe za obradom specijaliziranog jezika ulančanih blokova. Cilj rada je postaviti primjer dobre prakse u jezičnom upravljanju i planiranju kada je riječ o disruptivnim tehnologijama. Naime disruptivne tehnologije odlikuju se po naglom i snažnom utjecaju na tržište. Uslijed takvih naglih tehnoloških promjena vrijeme prilagodbe igra ključnu ulogu. Prilagodba se u ovom slučaju može smatrati prilagodba tradicionalnih tržišnih aktera na tržišne promjene, ali i prilagodba nekog društva ili jezične zajednice na disruptivnu tehnologiju. Ovladavanje terminologijom disruptivnih tehnologija unutar jezične zajednice omogućuje bržu prilagodbu i povećava potencijal iskorištavanja tehnologije u korist iste zajednice. Teresa M. Cabré na ovu temu piše:

> Terminološki rad povezan s jezičnim planiranjem za cilj ima ojačati i proširiti korištenje jezika, čineći ga iskoristivim u svim kontekstima. Iako mogućnost svakog jezika da opiše svaku specifičnu situaciju nije osporiva, društvene i gospodarske nejednakosti među državama omogućile su nekim jezicima da se razvijaju prirodno u toku s tehnološkim i komercijalnim razvojem, dok su drugi jezici u tome zaostajali. Jezik koji

[12] M. Teresa Cabré, Terminology: Theory, Methods and Applications, (John Benjamins Publishing Company, 1999.), 118.

se ne može koristiti u svim kontekstima osuđen je na nestanak, a jezik nije moguće koristiti ukoliko nema potrebnu terminologiju.[13]

Neosporivo je da se hrvatski nalazi među jezicima koji se spontano ne razvijaju dovoljno brzo u toku s globalnim tehnološkim i komercijalnim razvojem, te je ovakvo sistematsko razjašnjavanje i popisivanje termina jedan od načina koji mogu oplemeniti jezik i omogućiti korištenje jezika u novim tehnološkim kontekstima te obogatiti informatičku pismenost unutar jezične zajednice.

1.2. PREGLED LITERATURE

Nagli rast broja korisnika i sudionika u razvoju ovog sustava s otvorenim kodom, kao i dugogodišnji manjak interesa državnih i akademskih institucija, otvorili su prostor za veliku količinu pseudoznanstvenih tekstova na ovu temu iz nepouzdanih izvora informacija. U svrhu istraživanja terminologije ulančanih blokova ovaj će tekst koristiti isključivo formalne, pouzdane izvore informacija. Manjak akademskih tekstova u području istraživanja ulančanih blokova odraz je činjenice da su ulančani blokovi razmjerno nova tehnologija. Mnoštvo dostupnih izvora nalazi se u obliku bijelih knjiga napisanih u svrhu poslovnog ovladavanja ulančanim blokovima.

Bijela knjiga u području računarstva i informatike označava tekst kojim tvrtke za razvoj softvera tržišno pozicioniraju novu tehnologiju.[14] Funkcija bijele knjige znatno se razlikuje od funkcije klasičnog akademskog teksta, bijela knjiga nije uređena istim pravilima citiranja, stila i retorike kao i akademski tekst. No, to ne znači da bijele knjige nisu valjani izvor informacija te se kao takve u ovom radu koriste za razjašnjavanje tehničkih elemenata tehnologije kao i njene primjene. Po svojoj prirodi, bijele knjige bit će slabo teorijski pozicionirane te će rijetko čitatelja dovesti do nekog drugog relevantnog izvora. Stoga je važno pri njihovom korištenju također koristiti znanstvene članke i knjige koji nude teorijsku pozadinu. Prva i najvažnija bijela knjiga u ovom tekstu upravo je članak zaslužan za nastanak tehnologije ulančanih blokova. Riječ je o tekstu koji potpisuje Satoshi Nakamoto, pseudonim za autora ili skupina autora zaduženih za osmišljanje prve implementacije sustava ulančanih blokova, naslovljenom „*Bitcoin: A Peer-to-Peer Electronic Cash System*“. Bijela knjiga

[13] M. Teresa Cabré, Terminology: Theory, Methods and Applications, (John Benjamins Publishing Company, 1999.), 17, 18.
[14] Anthony James, Origin of White Papers (Klariti, 2017.), URL: http://klariti.com/white-papers/origin-of-white-papers/

bitcoina prvi je tekst ikada napisan na temu ulančanih blokova, a posjeduje svega osam citiranih izvora. Jasno je da tehnologija ulančanih blokova izgrađena na već oblikovanim temeljima matematike, kriptografije, informatike, upravljanja bazama podataka, digitalnog potpisivanja, ekonomije i trgovine. Ovu interdisciplinarnost nije lako iščitati iz bijelih knjiga, koje po svojoj prirodi ne razjašnjavaju kompleksne odnose tehnologije i znanja, već težište stavljaju na praktičnu primjenu i uporabu. Osim takozvane bijele knjige bitcoina, u tekstu je navedeno mnoštvo drugih bijelih knjiga, poglavito napisanih za projekte ulančanih blokova privatnih tvrtki i vladinih tijela raznih država. Veliki broj tekstova napisan je upravo od strane poduzetnika koji su ponukani uspjehom bitcoina sami razvili sustave alternativnih kriptovaluta. *Ethereum*, sustav razvijen na tehnologiji ulančanih blokova koji implementira virtualni stroj u ulančane blokove i time omogućuje pokretanje decentraliziranih aplikacija unutar mreže, prvi je puta također predstavljen u obliku bijele knjige. Autor Vitalik Buterin u ovom pogledu odskače od klasičnog oblika bijele knjige te nudi povijesni pregled tehnologije kao i detaljan opis kriptografskih elemenata sustava. Originalna bijela knjiga *Ethereuma* ne sadrži citirane izvore već na kraju teksta nudi izvore za dodatno čitanje.[15] Njen naknadni revidirani oblik na otvorenoj platformi *GitHub* sadrži sedamnaest citata, no platforma korisnicima nudi mogućnost mijenjanja teksta, što znači da revidirana verzija nema stalan oblik i nije dobar primarni izvor informacija.[16] Kao dobar i relevantan izvor u obliku bijele knjige u tekstu se javlja Izvještaj Ureda za znanost Vlade Ujedinjenog kraljevstva o tehnologiji distribuirane glavne knjige.[17] Nadalje u bijele knjige može se uvrstiti i vizualno atraktivni web sadržaj tvrtke Goldman Sachs, u kojem tvrtka iznosi svoje poimanje tehnologije.[18] Za razliku od akademske produktivnosti, produktivnost medija na temu ulančanih blokova izrazito je plodna. Zbog konteksta u kojem je nastala tehnologija ulančanih blokova, najveću pažnju tematici pridali su upravo ekonomski časopisi i novine. U tekstu se koriste izvori iz slijedećih periodičkih i internetskih izdanja: Economist, Harvard Business Review, New York Times, The Atlantic i Forbes. Kao izdašan izvor informacija na mreži javlja se i blog platforma Medium, unatoč tome što se radi o nelektoriranom i nekorigiranom

[15] Vitalik Buterin, Ethereum White Paper, URL: https://whitepaperdatabase.com/ethereum-eth-whitepaper/
[16] Vitalik Buterin, Ethereum White Paper, URL: https://github.com/ethereum/wiki/wiki/White-Paper
[17] UK Government Office for Science, Distributed Ledger Technology: beyond block chain, (UK Government report, 2017.)
URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
[18] Goldman Sachs, Blockchain – The New Technology of Trust, (Goldman Sachs, 2019)
URL: http://www.goldmansachs.com/our-thinking/pages/blockchain/

sadržaju. Stoga sadržaju na ovakvoj otvorenoj platformi treba pristupati kritički. U tekstu su navedeni isključivo blogovi koji zadovoljavaju kriterije znanstvenog pisanja te čiji autori pišu u skladu s pravilima dobre novinarske prakse.

Kao treća skupina izvora informacija javljaju se knjige publicističke prirode. Zanimljiva je činjenica da knjiga, za razliku od akademskih članaka, ima mnoštvo. Jedno objašnjenje za takav nerazmjer upravo je činjenica da se radi o vrlo popularnoj tehnologiji, te su izdavači prepoznali veliki interes javnosti za tematiku. Utrka za profitom uvjetovala je što ranije izdavanje knjiga, što je utjecalo na njihovu kvalitetu. Mnoge knjige o ulančanim blokovima dostupne na tržištu napisane su brzopleto i užurbano te obiluju greškama u pisanju, nekritičnom biranju izvora i senzacionalističkom preuveličavanju. Unatoč tome, dostupna literatura može ponuditi nove uvide u poimanje tehnologije i njenu terminologiju. Knjiga Dona i Alexa Tapscotta naslovljena „Revolucija ulančanih blokova: kako tehnologija na kojoj se temelji bitcoin mijenja novac, poslovanje i svijet“ reklamira se kao prva knjiga koja razjašnjava tehnologiju ulančanih blokova. Knjiga stavlja pretjerano težište na veličanje tehnologije, dok su tehnički aspekti u potpunosti zanemareni. Autori su ekonomisti, pa je nerealno očekivati detaljno poznavanje informatike ili kriptografije, no senzacionalizam i manjak kritičnosti jasno je vidljiv u tekstu. Knjiga Imrana Bashira, „Savladavanje ulančanih blokova“ tehnički je mnogo izdašnija. Bashir razjašnjava temelje tehnologije te nudi primjere programskog koda kao dodatni sadržaj uz knjigu. Knjiga sadrži opsežan popis terminologije ulančanih blokova, no loš stil pisanja i na mahove nejasan jezik umanjuju vrijednost ovog izvora. „Ulančani blokovi: jednostavan vodič za sve što trebate znati“ ambiciozan je naslov knjige Jacoba Williama koja obiluje anegdotalnim primjerima i mutnim analogijama. Manjak citiranja izvora, česte pravopisne pogreške i slaba logička povezanost između poglavlja ovu knjigu čine u najbolju ruku manjkavim izvorom informacija. Popularno poznata pod imenom „Princetonova knjiga o bitcoinu“ skupine autora sa Sveučilišta Princeton, svakako je najbolja i najopsežnija knjiga o ulančanim blokovima. Punog naziva „Bitcoin i tehnologije kriptovaluta“ ova knjiga izvorno je napisana u obliku serije besplatnih predavanja. Narayanan, Bonneau, Felten, Miller, Goldfeder i Clark donose iscrpan, tehnički potkovan i sažeti pregled tehnologije ulančanih blokova. Melanie Swan u knjizi „Ulančani Blokovi: Nacrt za novu ekonomiju“ donosi informativan i detaljan pregled tehnologije ulančanih blokova. Jedan izvor koji je bio posebno važan u pisanju ovog rada, i koji me naveo na odabir teme, svakako je

onaj međunarodnog istraživačkog projekta InterPARES Trust, u sklopu kojeg je razvijena jednojezična terminološka baza ulančanih blokova.[19]

Terminološka literatura, za razliku od one povezane s ulančanim blokovima, ustaljena je i utemeljena na godinama teoretske i praktične aktivnosti. Izbor knjiga na temu terminologije je širok, no među autorima posebno se ističe Theresa M. Cabré, u knjizi „Terminology: Theory, Methods and Applications“ objavljenoj 1999. vrlo jasno i koncizno razjašnjava teoriju i pristupe terminologiji, te čitatelja navodi na starija, prvotna terminološka djela kao što su Wüsterov „Uvod“ i Augerova „Metodologija“. Nadalje „Encyclopedia of translation studies“ nakladne kuće Routledge izvrstan je izvor za definiranje osnovnih pojmova unutar terminografije. Nadalje, kao vodič za pristup terminologiji unutar jezične zajednice, izrazito je koristan UNESCO-v dokument „Smjernice za terminološke politike: oblikovanje i provedba terminološke politike u jezičnim zajednicama“. Ovaj dokument u detalje razjašnjava stav UNESCO-a prema jezičnim politikama i jezičnom planiranju, na koje se poziva i ovaj rad kako bi opravdao i naglasio jezičnu potrebu za razvojem terminologije svih disruptivnih tehnologija pa tako i one ulančanih blokova. Daljnja rasprava o teoriji terminologije nalazi se u poglavlju 3, naslovljenom Terminologija i terminografija.

[19] InterPARES Trust, Blockchain terminology (2018.) URL: https://interparestrust.org/terminology/term/blockchain

2. TEHNOLOGIJA ULANČANIH BLOKOVA

Tehnologija ulančanih blokova disruptivna je računalna tehnologija koja se zasniva na konceptu distribuirane glavne knjige. Distribuirana glavna knjiga, odnosno *distributed ledger* na engleskom, u stvari je mrežna baza podataka s otvorenim pristupom kojoj mogu pristupati i koju mogu ažurirati svi umreženi sudionici.[20] Prijenos podataka i informacija je trenutan, te se točnost podataka kontrolira kriptografski.[21] U svrhu preciznijeg opisivanja osnovnog pojma, potrebno je sagledati razne definicije ulančanih blokova koje nude stručnjaci. Jedna od četiri najveće konzultantske tvrtke, KPMG ulančane blokove definira kao „bazu podataka u obliku distribuirane glavne knjige koja čuva stalno rastuću količinu zapisa o transakcijama poredanih u blokove zaštićene od falsifikacije i naknadnog mijenjanja.“[22] Deloitte pak ulančane blokova smatra „generičkim imenom za obitelj tehnologija koje nude istu funkcionalnost kao bitcoin, no koje koriste različiti pristup u realizaciji tih funkcionalnosti, koristeći različite algoritme.“[23] Tvrtka PWC ulančane blokova definira na slijedeći način: „Ulančani blokovi su distribuirana glavna knjiga svih transakcija unutar mreže, koja decentralizira povjerenje i omogućuje protok vrijednosti bez posrednika.“[24] Tvrtka Ernst & Young, ulančane blokove pak definira ovako: „Ulančani blokovi su vrsta baze podataka koja bilježi rastući popis nepromjenjivih zapisa, tzv. blokova.“[25] U uvodnom poglavlju ovog rada navedene su još neke definicije ulančanih blokova iz publicističke literature, od kojih ni jedna nije potpuna. Opća definicija ulančanih blokova može se sastaviti od elemenata svih navedenih definicija. Ulančani blokovi u svakom su slučaju distribuirana glavna knjiga, koja se ponekad opisuje i kao baza podataka. U svakoj definiciji opisan je način zapisivanja podataka u tu glavnu knjigu, naime važno je da su podaci logički organizirani u blokove, te da su kriptografski osigurani. Neke definicije spominju transakcije, dok druge govore isključivo o čuvanju zapisa

[20] David Mills et al., Distributed ledger technology in payments, clearing, and settlement (Federal Reserve, 2016), 12
URL: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf
[21] Economist, Blockchains: The great chain of being sure about things, (Economist, 2015.)
URL: https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things
[22] George Samman, Sigrid Seibold, Consensus: Immutable agreement for the Internet of Value (KPMG, 2018.), 2.
URL: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf
[23] Deloitte Centre for the Edge, Australia, Bitcoin, Blockchain and distribueted ledgers, caught between promise and reality, (Deloitte, 2018.), 9.
URL: https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf
[24] PWC, Blockchain Overview (PWC, 2018.)
URL: https://mytaxpartner.pwc.com/media/1247992/blockchain-overview.pdf
[25] Angus Champion de Crespigny, Blockchain: the hype, the opportuinty and what you should do, (EY, 2018.), 2.
URL: http://www.ey.com/Publication/vwLUAssets/ey-blockchain-the-hypethe-opportunity-and-what-you-should-do/ %24FILE/ey-blockchain-the-hypethe-opportunity-and-what-you-should-do.pdf

u širem smislu. U ovom slučaju, za definiciju je prikladniji pojam šireg značenja, kako sama definicija ne bi limitirala poimanje primjene tehnologije. Veliki je naglasak na nekrivotvorivosti i nepromjenjivosti zapisa unutar ulančanih blokova, što je jedna od ključnih funkcionalnosti sustava. Ulančani blokovi su dakle baza podataka u obliku distribuirane glavne knjige u kojoj se bilježe nepromjenjivi zapisi organizirani u kriptografski osigurane blokove. Ovo će poglavlje pomnije opisati ulančane blokove, njihove tehničke aspekte i obilježja, povijest i razvoj ove tehnologije te interdisciplinarnost iste kao i potencijalne primjene ulančanih blokova.

2.1. TEHNIČKI ASPEKTI I OBILJEŽJA

Glavna knjiga kao pojam iz računovodstva označava dokument koji bilježi zapise o poslovanju nekog poduzeća. Distribuirana glavna knjiga decentralizirani je način čuvanja zapisa u kojem više entiteta podatke može upisivati u glavnu knjigu. U ovom slučaju atribut distribuiranosti proizlazi iz decentralizirane prirode sustava, sva računala na mreži mogu upisivati podatke u glavnu knjigu. Lanac blokova u stvari je kriptografski zapisana glavna knjiga, organizirana u blokove koji povezani čine logički lanac. Takav lanac blokova omogućuje dugoročno čuvanje zapisa upisanih u distribuiranu glavnu knjigu bez mogućnosti mijenjanja i ažuriranja postojećih zapisa. Potpuna otvorenost sustava postiže se kriptografskim konsenzusom. Opisujući bitcoin sustav, Narayanan et al. poistovjećuju ulančane blokove i distribuirani glavnu knjigu: „još jedna ključna komponenta Bitcoina su ulančani blokovi: glavna knjiga koja na siguran način bilježi transakcije.“ Taj siguran način bilježenja ovaj sustav postiže mješavinom kriptografije, logičkog slijeda podataka i vremenskih oznaka. [26]

U distribuiranom otvorenom sustavu, kao što je lanac blokova, kriptografija osigurava integritet glavne knjige, autentičnost zapisa u njoj, povjerljivost pri upisivanju podataka u lanac te jedinstveni identitet sudionika u mreži. Svaki blok u lancu u stvari je skup zapisa kriptiranih funkcijom SHA-256. SHA-256, punim nazivom *Secure Hash Algorithm,* je kriptografska funkcija za sažimanje (eng. *crpytographic hash function*) koja određeni tekstualni unos pretvara u hash vrijednost. Hash vrijednost je niz brojeva i znamenki jedinstven za svaki unos. Iz hash vrijednosti nije moguće rekonstruirati originalni zapis, no vlasnik originalnog zapisa može provjeriti točnost jedinstvene hash vrijednost u bloku. Na taj se način osigurava transparentnost, povjerljivost i pristup podacima. Hash vrijednost je

[26] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfede, Bitcoin and Cryptocurrency Technologies (Princeton University Press, 2016.), 15

jedinstvena jer čak i najmanja promjena informacije pri unosu potpuno mijenja zapis. Narayanan et al. definiraju kriptografsku funkciju za sažimanje adekvatnu za sustav ulančanih blokova kao matematičku funkciju koja zadovoljava nekoliko kriterija. Na primjer, kriptografska funkcija za sažimanje mora podržavati ulaznu vrijednost neograničene veličine, što omogućuje da se u ulančane blokove spremaju sve vrste digitalnih zapisa, neovisno o njihovoj veličini. Nadalje, ulazna vrijednost proizvodi izlaznu vrijednost predodređene veličine, u slučaju enkripcijom funkcijom SHA-256, riječ je o zapisu veličine 256 bita. Kriptografska funkcija u sustavu ulančanih blokova mora ulaznu vrijednost brzo preračunati u izlaznu, odnosno kriptografska funkcija za sažimanje u kontekstu ulančanih blokova mora biti lako izračunljiva. Osim što mora imati gore navedene funkcije, kriptografska funkcija za sažimanje mora biti otporna na koliziju, tj. dva različita ulaza ne smiju proizvesti jednaku izlaznu vrijednost. Kriptografska funkcija za sažimanje k tome mora biti i skrivajuća, ako je $y = hash(x)$ onda nije moguće izračunati vrijednost x iz vrijednosti y. Zadnje svojstvo koje kriptografska funkcija za sažimanje mora podržavati mogućnost postavljanja kriptografske zagonetke (eng. *puzzle friendliness*). To svojstvo izrazito je važno za konsenzusne protokole opisane u nastavku teksta.[27]

Lanac blokova grade računala spojena u *peer-to-peer* mrežu. Računala koja sudjeluju u izgradnji lanca u mreži mogu služiti kao čvor (eng. *node*) ili rudar (eng. *miner*). Čvor je svako računalo na mreži koje čuva kopiju cijelog lanca blokova i provjerava točnost novih zapisa odobravajući ih ili odbijajući. Konsenzus se postiže prihvaćanjem novog bloka od strane kvalificirane većine (50 % plus 1) čvorova na mreži. Kod nekih konsenzusnih mehanizama, uobičajeno kad je riječ o kriptovalutama, novi blokovi nastaju rudarenjem. U mreži ulančanih blokova rudari su računala koja koriste procesorsku snagu za izračun novog bloka i stjecanje kripto-vrijednosti. Samo čvor koji je prvi izračunao traženu vrijednost drugim čvorovima predlaže novi blok. To je moguće postići uz korištenje velike količine procesorske snage, najčešće međusobno povezanog velikog broja grafičkih kartica. Takav pristup, utemeljen na konceptu dokaza o radu (eng. *proof-of-work*) omogućava stjecanje virtualne vrijednosti, kao što je to bitcoin, jer se u zamjenu za dokaz o radu dobiva kriptovaluta. Postoje i konsenzusni mehanizmi distribuirane glavne knjige koji ne zahtijevaju dokaz o radu, jer nije cilj stjecanje virtualne vrijednosti..

[27] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfede, Bitcoin and Cryptocurrency Technologies (Princeton University Press, 2016.), 10-17

Računala u funkciji čvorova nadalje mogu biti djelomični čvorovi (eng. *partial node*) i potpuni čvorovi (eng. *full node*). Imran Bashir čvorove unutar ulančanih blokova opisuje na slijedeći način: „Čvor u mreži ulančanih blokova vrši razne funkcije ovisno o ulozi koju preuzima. Čvor može predlagati i potvrđivati transakcije, rudariti kako bi se ojačao konsenzus i osigurali ulančani blokovi. To se postiže konsenzusnim protokolom (najčešće protokolom PoW). Čvorovi također mogu vršiti druge funkcije, na primjer jednostavno potvrđivanje uplata, provjeravanje i mnoge druge funkcije ovisno o vrsti ulančanih blokova i ulozi koja je pridana čvoru.“[28] Korisnik koji želi sudjelovati u izgradnji ulančanih blokova na svoje će računalo instalirati željeni softver čijim će pokretanjem spojiti svoje računalo na mrežu i započeti vršiti određenu funkciju unutar mreže.

Povjerenje u sustav ulančanih blokova postiže se distribuiranim konsenzusom računala spojenih na mrežu. Pojam „konsenzus“ u ovom kontekstu prelazi svoje opće jezično značenje. Budući da svaki entitet spojen na mrežu može pohranjivati podatke u lanac blokova, neophodno je da najmanje kvalificirana većina distribuiranih učesnika provjeri podatke i slože se s njihovim upisivanjem u lanac. U umreženim sustavima to se postiže konsenzusnim algoritmima čiji je cilj onemogućiti neovlašteno upisivanje podataka ili dvostruke transakcije (eng. *double spending*). Povjerenje u distribuirani konsenzus proizlazi iz tzv. bizantske tolerancije na pogreške (eng. Byzantine fault tolerance). Naime svaki sustav koji koristi distribuirani konsenzus mora riješiti tzv. problem bizantskih generala (eng. Byzantine Generals Problem). U otvorenom (eng. *premissionless*) sustavu ulančanih blokova konsenzus se može postići pomoću raznih algoritama. Najuspješniji konsenzusni algoritmi trenutno su: dokaz o radu (eng. Proof of Work, PoW) i dokaz o ulogu (eng. Proof of Stake, PoS). U zatvorenom (eng. *permissioned*) sustavu konsenzus se ne mora utvrđivati pomoću konsenzusnih algoritama, već administrator kontrolira broj računala u mreži koja će konsenzusom donositi odluke dok u otvorenom (eng. premissionless) bilo koje računalo se može priključiti i sudjelovati u donošenju konsenzusa. Također se razlikuju i javni (eng. *public*) i privatni (eng. *private*) sustavi ulančanih blokova. Dakle, razlika je u tome da u otvorenim sustavima nije potrebno dobiti autorizaciju za upisivanje podataka u ulančane blokove, dok u zatvorenim sustavima korisnici moraju imati autorizaciju, u javnom sustavu ulančanih blokova pak mogu prisustvovati svi, dok u privatnim mogu sudjelovati samo računala pozvana u mrežu.

[28] Imran Bashir, Deeper insights into decentralization, cryptography, Bitcoin and popular Blockchain frameworks, (Packt, 2017)

Problem bizantskih generala klasična je logička zagonetka u kojoj skupina bizantskih generala opsjeda neki grad. Svaki general zapovijeda dijelom vojske, te generali komuniciraju putem poruka kako bi razvili zajednički plan napada. Među njima je određeni broj izdajnika, koji namjerno mogu sabotirati dogovore. Cilj je da se korištenjem matematike postigne da svi lojalni generali napadnu u isto vrijeme, bez da ih izdajnički generali nagovore na loš plan. Matematički je dokazano da konsenzus u ovakvom slučaju nije moguć ako je više od jedne trećine izdajničkih generala.[29] Svaki sustav ulančanih blokova koji se zasniva na distribuiranom konsenzusu mora ponuditi rješenje za ovaj problem, te pokazati da sustav ima Bizantsku toleranciju na pogreške. U sustavu ulančanih blokova računala zauzimaju mjesto generala, dok je dogovor o planu napada u stvari konsenzus o upisivanju podataka u ulančane blokove. Maliciozna računala ne smiju moći omesti rad benevolentnih računala kako bi se postigao distribuirani konsenzus.

Algoritam Dokaz o radu kriptografska je zagonetka koja služi kao dokaz da je neko računalo utrošilo procesorski kapacitet kako bi došlo do rješenja. Algoritam su 1999. godine predložili Jakobson i Juels kao mjeru sprječavanja nepoželjnih *spam* e-mailova.[30] U sustavu ulančanih blokova algoritam Dokaz o radu od rudarskih računala iziskuje izračun jednokratnog kriptografskog izraza (eng. *nonce*) prema pravilima mreže. Za rješavanje jedne kriptografske zagonetke potrebna je golema količina procesorske snage nekog računala. Vrijednost jednokratnog kriptografskog izraza definirana je pravilima koja tu vrijednost čine izrazito vremenski zahtjevnom za izračunati. Ovaj mehanizam zahtjeva da rudar koji upisuje novi blok u lanac utroši pozamašnu količinu procesorske snage, no i sprječava naknadno mijenjanje zapisa upisanih u lanac. Kako bi se već upisani zapis promijenio, maliciozni akter mora ponuditi novi izračun jednokratnog kriptografskog izraza za blok koji mijenja, kao i za svaki prijašnji blok u lancu. Budući da je za svaki postojeći blok već ponuđen Dokaz o radu u obliku jednokratnog kriptografskog izraza i činjenice da lanac stalno raste, procesorska snaga utrošena za mijenjanje zapisa u lancu mora biti veća od one utrošene u izračunavanje svih blokova nastalih nakon promijenjenog bloka. U otvorenom sustavu to znači da maliciozni akter mora posjedovati više od 50 % procesorske snage u cijeloj mreži, a u zatvorenom sustavu kontrolirati više od 50 % računala kako bi izgradio najdulji lanac blokova. Time bi mogao preuzeti kontrolu nad daljnjim razvojem lanca blokova, ali i dalje ne bi mogao

[29] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfede, Bitcoin and Cryptocurrency Technologies (Princeton University Press, 2016.), 45
[30] Markus Jakobson, Ari Juels, Proofs of work and bread pudding protocols (extended abstract) (Bell Labs, RSA, 1999.)
URL: http://www.hashcash.org/papers/bread-pudding.pdf

mijenjati ono što je do tog trenutka zapisano i bilo potvrđeno kao istina od strane svih ostalih čvorova.

Kao alternativa algoritmu Dokaza o radu javlja se Dokaz o ulogu. Naime Dokaz o radu konsenzusni je algoritam koji znatno usporava rast ulančanih blokova. Vremenski manje zahtjevna alternativa, Dokaz o ulogu temelji se na slijedećem principu: „U ovoj shemi ideja je da korisnici moraju dokazati vlasništvo nad određenom količinom kriptovalute, time dokazujući da imaju ulog u sustavu. Najjednostavniji oblik algoritma je onaj u kojem je rudarenje olakšano onim korisnicima koji imaju dokazano vlasništvo nad većom svotom digitalne valute. Prednost ove sheme je dvojaka: pribavljanje velike količine digitalne valute putem rudarenja je relativno teško i rezultira štednjom računalnih resursa.“[31]

Svi navedeni elementi zajedno čine sustav ulančanih blokova u kontekstu kriptovaluta, čija se logička struktura zasniva na povezanosti između kriptografskih jedinica – blokova. Blok je naime niz zapisa kriptiranih u jednu cjelinu s nekim dodanim informacijama. Imran Bashir blok opisuje ovako: „Blok se sastoji od više transakcija i drugih elemenata kao što su hash vrijednost prijašnjeg bloka, hash pokazivač, vremenska oznaka i jednokratni kriptografski niz.“[32] Svaki blok u sebi ima zapisanu hash vrijednost prijašnjeg bloka. Ta vrijednost u stvari ima funkciju povezivanja uzastopnih blokova u slijed. Hash vrijednost prijašnjeg bloka ima funkciju pokazivača jer pokazuje koji blok dolazi prije trenutnog bloka, time se osigurava točan raspored blokova te onemogućava naknadno mijenjanje zapisa u ulančanim blokovima. Narayanan et. al pišu: „Hash pokazivač je jednostavan pokazivač koji pokazuje gdje se nalazi informacija, uz kriptografsku hash vrijednost te informacije. Dok obični pokazivač nudi mogućnost pronalaska informacije, hash pokazivač također omogućuje da provjerite je li informacija promijenjena.“[33] Sve informacije pridodane bloku bilježe se u zaglavlje bloka (eng. *block header*). Osim hash pokazivača u bloku se nalaze kriptirane informacije u obliku Merkleovog stabla. Na primjer, sustav ulančanih blokova koje koristi Bitcoin u blokove bilježi hash vrijednosti novčanih transakcije. Svaka transakcija se u lancu prikazuje kao jedinstvena hash vrijednost. Iz te hash vrijednosti ne može se zaključiti identitet sudionika ni vrijednost transakcije, no sudionici posjeduju dokaz da je transakcija obavljena.

[31] Imran Bashir, Deeper insights into decentralization, cryptography, Bitcoin and popular Blockchain frameworks, (Packt, 2017)
[32] Imran Bashir, Deeper insights into decentralization, cryptography, Bitcoin and popular Blockchain frameworks, (Packt, 2017)
[33] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfede, Bitcoin and Cryptocurrency Technologies (Princeton University Press, 2016.), 45

No, neopreznim korištenjem kriptovaluta moguće je doznati identitet korisnika.[34, 35] Kada se u jednom bloku zabilježi dovoljan broj transakcija ili kad prođe određeno vrijeme između formiranja dvaju blokova zadano sustavom, sve novozaprimljene hash vrijednosti zajedno s hash vrijednošću prethodnog bloka koja u sebi sadrži hash vrijednosti prijašnjih blokova, kriptiraju se istom funkcijom, čime se dobiva jedinstvena hash vrijednost cijelog bloka. Logičkim slijedom blokova u kojem svaki novi blok sadrži hash vrijednost svih prijašnjih blokova omogućava se dugoročno, sigurno čuvanje zapisa o transakcijama. Takav logički slijed hash vrijednosti naziva se Merkleovim stablom. Merkleovo stablo kriptografski je alat koji omogućuje sigurnu i brzu provjeru sadržaja velike količine podataka.[36] Blok se, dakle, sastoji od hash vrijednosti zapisa i zaglavlja u kojem se nalazi hash vrijednost prijašnjeg bloka, hash pokazivač i vremenska oznaka.

U sustavu ulančanih blokova razlikujemo više vrsta blokova. Prvi blok u ulančanim blokovima naziva se inicijalnim blokom (eng. *genesis block*). Budući da prvom bloku ne možemo pridodati hash pokazivač na prijašnji, u njega umjesto hash pokazivača bilježimo neku arbitrarnu informaciju koja će služiti kako bi dali vremenski kontekst pokretanju sustava. Pri izradi inicijalnog bloka provenijencija je neupitna jer inicijalni blok rudari računalo koje kontrolira autor sustava.

2.2. POVIJEST I RAZVOJ ULANČANIH BLOKOVA I KRIPTOVALUTA

Povijest ulančanih blokova relativno je kratka, tehnologija je svijetu predstavljena 2008. godine. No ta tehnologija nije nastala u vakuumu, ona je plod ideja i tehnoloških izuma usko povezanih s razvojem informatike i računarstva. Ključni trenutak u povijest ulančanih blokova kreacija je bitcoina, no bitcoin nije prvi digitalni novac, te su povijest ulančanih blokova i povijest digitalnog novca usko povezani. U svrhu povijesnog pregleda tehnologije ulančanih blokova ovo će poglavlje biti podijeljeno na dva dijela - prvi će se baviti idejnim i

[34] Vidi: How can I trace a Bitcoin wallet owner using their wallet address?, https://www.quora.com/How-can-I-trace-a-Bitcoin-wallet-owner-using-their-wallet-address
[35] Vidi: Top Seven Ways Your Identity Can Be Linked to Your Bitcoin Address, https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/
[36] Georg Becker, Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis, (Ruhr-Universitat Bochum, 2008.), 12
URL:http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/becker_1.pdf

tehnološkim pretečama koje su omogućile nastanak ove tehnologije, dok će drugi sagledati razvoj tehnologije nakon njenog nastanka.

Narayanan et. al prepoznaju dva koncepta ključna u razumijevanju nastanka ulančanih blokova, od kojih je prvi zajednica *cypherpunk. Cypherpunk* je neformalna zajednica koja je 1990-ih godina postojala u obliku liste za e-mail. Unutar te zajednice vodile su se rasprave o korištenju kriptografije kao rješenju za sigurnost i privatnost pojedinaca na mreži. Osim uvjerenja u boljitak putem tehnologije, zajednica je prihvatila ideje libertarijanizma, koji prema autorima čini drugi ključni koncept.[37] Jedna od ideja nastala aktivnostima te zajednice bila je decentralizirana valuta u obliku digitalnog novca, koja bi korisnicima omogućila sigurne i anonimne transakcije neovisne o državi i njenim financijskim institucijama. Bitcoin, prva tehnologija ulančanih blokova, jasno odražava te ideološke osnove nastale putem e-mail komunikacije. Bitcoin nije prvi pokušaj stvaranja digitalne valute, te je povijest digitalnog plaćanja istovjetna povijesti povjerenja i sigurnosti na internetu. Ulančani blokovi predstavljaju rješenje tog problema povjerenja i sigurnosti, te je za razumijevanje tehnologije potrebno poznavanje njenih korijena.

Jedna od tehnoloških preteča tehnologiji ulančanih blokova nalazi se u članku „Kako vremenski označiti digitalni dokument“, gdje je predstavljena shema razvijena 1991. godine koja sažima skupine podataka u blokove, međusobno ih povezuje u lanac i označava vremenskom oznakom. Haber i Stornetta predložili su sustav koji blokove povezuje pomoću hash pokazivača (eng. *hash pointer*), svaki blok u lancu sadrži hash vrijednost prijašnjeg bloka te se time rješava problem vremenskog rasporeda nastanka digitalnih dokumenata. Nadalje u blokovima se nalaze podaci kriptirani i raspoređeni u obliku Merkleovog stabla, što omogućuje da se u jednom bloku nalaze zapisi više digitalnih dokumenata. Svi suvremeni sustavi ulančanih blokova koriste ovu logičku shemu sustava. [38]

David Chaum osmislio je prvi sustav digitalnog plaćanja 1989. godine kada je osnovao tvrtku DigiCash. Tvrtka je razvila usluge anonimnog transfera novca koristeći uslugu Ecash, koja je nudila mogućnost transakcija u dolarima. Ideja anonimnosti u internetskom plaćanju izrazito je važna u razvoju ulančanih blokova te se kao ključna ideja održala sve do danas, a

[37] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfede, Bitcoin and Cryptocurrency Technologies (Princeton University Press, 2016.), 45
[38] Stuart Haber, W. Scott Stornetta, How to Time-Stamp a Digital Document,(Autoridad de Certificacion, 1991.), URL: https://crl.anf.es/pdf/Haber_Stornetta.pdf

David Chaum smatra se pionirom anonimne komunikacije.[39] Godine 1994. tvrtka FirstVirtual usporedno je razvila sustav digitalnog plaćanja izravno koristeći kreditne kartice. Korisnici su tvrtki povjerili podatke svojih kreditnih kartica, internetskoj bi trgovini povjerili svoj identifikacijski broj, te bi trgovina zatim kontaktirala FirstVirtual. Sve transakcije potvrđivale su se putem e-maila, budući da je to prije razvitka sigurnosnih protokola bio najsigurniji način komunikacije putem interneta. Tvrtka je zaustavila svoje aktivnosti 1998. godine, no sustav posredovanja pri internetskom plaćanju ostat će jedina sigurna opcija još dugi niz godina.[40] U isto vrijeme tvrtka CyberCash pokušala je razviti sustav internetskog plaćanja koristeći neke inovativne ideje, posebno su zanimljivi nazivi proizvoda i usluga koje je CyberCash nudio korisnicima. Naime, suvremena terminologija ulančanih blokova može se izravno povezati s uslugama koje je 1996. prvi puta ponudio CyberCash. CyberCash je kao uslugu nudio prvu digitalnu valutu po imenu CyberCoin, koja je tada korištena za mikrotransakcije, a svaki korisnik imao je vlastiti digitalni novčanik, zaštićen tada naprednom kriptografijom. Sustav nije zaživio, no ideja o čuvanju digitalnih novčića u kriptografski zaštićenom korisničkom računu, to jest novčaniku, ostavština je tvrtke CyberCash.[41]

Programer Adam Back je 1997. osmislio računalnu kriptografsku zagonetku na kojoj se danas zasniva bitcoin. Hashcash je sustav izvorno osmišljen kako bi spriječio slanje velike količine neželjenih, spam e-mailova. Back je osmislio prvi sustav dokaza o radu (eng. *proof-of-work*), gdje je računalo moralo riješiti kriptografsku zagonetku koja je bila vremenski zahtjevna za procesirati. Bio je to pokušaj da se učini nepraktičnim slanje velike količine e-mailova na različite adrese.[42] Sustav nije zaživio u ovoj funkciji, no identičnu zagonetku koriste ulančani blokovi bitcoina pri rudarenju. Godine 1998. Wei Dai informatičar kineskog podrijetla, napisao je prijedlog za digitalnu valutu, Dai piše: „Zajednicu definira suradnja svih članova, a efikasna suradnja zahtjeva medij razmjene (novac) i način da se provedu ugovori. Tradicionalno te usluge nudi država ili državna institucija isključivo pravnim osobama. U ovom članku opisujem protokol u kojem te usluge nude i koriste anonimni entiteti.“[43] Protokol kojeg Dai opisuje nosi ime b-money, a zasniva se na sustavu povezanih računala

[39] David Chaum, World's first electornic cash payment over computer networks, (David Chaum, 1992.)
URL: https://chaum.com/projects/eCash
[40] PCMag, First Virutal, (1998.)
URL: https://www.pcmag.com/encyclopedia/term/43226/first-virtual
[41] CNet, CyberCash open Net to small change, (1996.),
URL: https://www.cnet.com/news/cybercash-opens-net-to-small-change/
[42] Adam Back, Hashcash, (1997.)
URL: http://hashcash.org/docs/hashcash.txt
[43] Wei Dai, B-money, (1998.)
URL: http://www.weidai.com/bmoney.txt

koja sama tiskaju novčanice koristeći procesorsku snagu svojih računala. Dokaz o iskorištenoj procesorskoj snazi u stvari je rješenje neke kriptografske zagonetke. U sustavu koji je osmislio Dei svako računalo na mreži zasebno bilježi transakcije. Još jednom pretečom bitcoina smatra se bitgold, čiji autor Nick Szabo u svom blogu ovako opisuje sustav: „Stoga, bilo bi lijepo kada bi postojao protokol kojim bi se mogli stvarati nekrivotvorivi skupocjeni nizovi podataka na mreži s minimalnom ovisnosti o trećoj strani, koji bi se mogli sigurno čuvati, prenositi i provjeriti s minimalno povjerenja.“[44]

Razvojem sigurnosnih protokola na internetu potreba za posredničkom uslugom pri internetskom plaćanju postala je sve manja. Usluga PayPal javlja se kao rješenje za manjak povjerenja u razmjeni dobara i usluga za novce s nepoznatim ljudima na mreži. No izravno plaćanje kreditnim karticama i PayPal nisu osigurali anonimnost i privatnost, što je ostavilo prostora na tržištu internetskog plaćanja. U tom praznom prostoru javlja se bitcoin, prva internetska valuta koja korisnicima omogućava anonimni prijenos novca između računa bez centralne institucije. Bitcoin je idejni nasljednik ranije spomenutih pokušaja stvaranja digitalnih valuta. Bijela knjiga bitcoina napisana je 2008. godine, dok je prvi blok u lanac zabilježen 3. siječnja 2009. Za vremensku referencu, ali vjerojatno i kao ideološki komentari, u taj prvotni blok kriptografski je upisan naslov iz novina The Times „Kancelar na rubu drugog spašavanja banaka.“[45, 46] Godina 2009. označava početak razvoja ulančanih blokova kao tehnologije, ali i kriptovaluta kao ometajuće pojave na tržištu.

Sve do 2011. bitcoin je jedini sustav koji koristi ulančane blokove, no u 2011. godini javljaju se alternativne kriptovalute (eng. *altcoin*).[47] S alternativnim kriptovalutama javlja se i shvaćanje da se tehnologija na kojoj se temelji bitcoin može koristiti i izvan okvira digitalnih valuta. Vinay Gupta u svom članku o povijesti ulančanih blokova za *Harvard Business Review* piše: „Prva velika inovacija u polju ulančanih blokova bio je bitcoin, eksperimentalna digitalna valuta. Tržišna vrijednost bitcoina danas iznosi između 10 i 20 milijardi dolara, za online plaćanje bitcoin koriste milijuni ljudi, uključujući i rastuće tržište međunarodne isplate doznaka. Druga inovacija poznata je pod nazivom ulančani blokovi, kada se u stvari razvilo shvaćanje da se temeljna tehnologija na kojoj funkcionira bitcoin može razdvojiti od same

[44] Nick Szabo, Bit Gold (Blog, 2008.)
URL: https://unenumerated.blogspot.hr/2005/12/bit-gold.html
[45] EN: The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.
[46] Francis Elliot, Chancellor Allistair Darling on brink of second bailout for banks, (The Times, 2009.)
URL: https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h
[47] Javier Espinoza, Is It Time to Invest in Bitcoin?, (The Wall Street Journal, 2014.)
URL: https://www.wsj.com/articles/how-to-decipher-cryptocurrencies-1411333011

valute i koristiti u razne svrhe međuorganizacijske suradnje.“[48] Melanie Swan taj prijelaz smatra prekretnicom, a tu prekretnicu opisuje ovako: „Ulančani blokovi 1.0 su valute, razvoj kriptovaluta i primjena povezana s gotovinom, kao što je slanje i primanje valuta, slanje doznaka i sustavi digitalnog plaćanja. Ulančani blokovi 2.0 su ugovori, cijeli spektar ekonomske, tržišne i financijske primijene koristeći ulančane blokove na ekstenzivniji način od čistih gotovinskih transakcija: dionice, obveznice, kupoprodajni ugovori s odgođenom isporukom (eng. *futures*), zajmovi, hipoteke, vlasništvo, pametno vlasništvo i pametni ugovori. Ulančani blokovi 3.0 primjena su ulančanih blokova izvan valuta, financija i tržišta – posebice u području državne uprave, zdravstva, znanosti, pismenosti, kulturi i umjetnosti.“[49] Razvojem alternativnih kriptovaluta, narativa ulančanih blokova prvi se puta odvaja od bitcoina.

Alternativne kriptovalute golemo su tržište čije razjašnjavanje zahtjeva više prostora no što ovaj rad može ponuditi, no važno je spomenuti ih u kontekstu razvoja tehnologije ulančanih blokova. Neke od alternativnih kriptovaluta imaju istu funkciju kao i bitcoin - to su digitalne valute čiji je glavni cilj omogućiti korisnicima razmjenu vrijednosti, no neke alternative bitcoinu ponudile su sasvim novi uvid u tehnologiju. Alternativna kriptovaluta Namecoin, nastala 2011. za cilj ima popisivanje i čuvanje podataka o vlasništva nad internetskim domenama, nudeći tako alternativu DNS usluzi.[50] Ethereum je na svojevrstan način 2013. godine revolucionalizirao ulančane blokove omogućivši pisanje pametnih ugovora kao osnovnu uslugu. Steemit je usluga pametnog medija (eng. *smart media*) utemeljena 2016. koja, koristeći ulančane blokove, autorima isplaćuje nagrade za kreativni sadržaj u obliku kriptovalute Steem.[51] IOTA, alternativna kriptovaluta namijenjena komunikaciji između uređaja spojenih na internet, nastala je 2015. godine.[52]

Povijest ulančanih blokova ukazuje na šarenu i zanimljivu pozadinu koja je omogućila razvoj ove tehnologije. Ulančani blokovi razvili su se na raskršću mnoštva ekspertnih polja, tehnoloških otkrića i političkih ideala, koji svi skupa ovu tehnologiju čine interdisciplinarnom i njene primjene raznolikima. Iduća dva potpoglavlja pozabavit će se upravo interdisciplinarnošću ove tehnologije i širokim mogućnostima njene primjene.

[48] Vinay Gupta, A Brief History of Blockchain (Harvard Business Review, 2017.), URL: https://hbr.org/2017/02/a-brief-history-of-blockchain
[49] Melanie Swan, Blockchain: Blueprint for a New Economy (O'Reily, 2015.), 17
[50] Vidi: https://namecoin.org/
[51] Vidi: https://steem.io/
[52] Vidi: https://iota.org/

2.3. INTERDISCIPLINARNI TEMELJI TEHNOLOGIJE ULANČANIH BLOKOVA

Tehnologija ulančanih blokova razvila se na interdisciplinarnim temeljima, što se odražava na interpretaciju njene provenijencije i uporabe. Ulančani blokovi primarno su informatička tehnologija, razvijena za računalne i mrežne sustave. Najuspješnija dosadašnja primjena tehnologije svakako je internetska valuta Bitcoin, što omogućuje shvaćanje ulančanih blokova u širem smislu kao ekonomske, a u užem kao financijske tehnologije (eng. *fintech*). Ulančani blokovi nerazdvojni su, kako terminološki tako i tematski, od kriptografije, te je nemoguć razvoj sustava ulančanih blokova bez temeljitog poznavanja matematike. Razvijeni u svrhu bilježenja transakcija, ulančani blokovi ustvari su tehnologija dugotrajnog čuvanja zapisa, te se mogu interpretirati kao arhivska tehnologija, jer je njihov eksplicitni cilj na siguran i povjerljiv način čuvati podatke. Jedna od potencijalno najvažnijih primjena ove tehnologije leži u komunikaciji između uređaja povezanih na mrežu, te su u kontekstu *Internet of Things* (IoT) ulančani blokovi potencijalna tehnologija za sigurnu komunikaciju, što ulančane blokove podređuje pojmu kibernetske sigurnosti (eng. *cyber-security*).

Ulančani blokovi u svojoj su srži računalna to jest informatička tehnologija. Svaki sustav ulančanih blokova utemeljen je na programskom jeziku te razvoj i rad na ulančanim blokovima zahtjeva znanje programiranja. Osim tradicionalnih programskih jezika na kojima su ulančani blokovi izgrađeni, u svrhu njihove nadogradnje posebno su osmišljeni novi programski jezici. Sustav ulančanih blokova bitcoin za osnovu koristi C++, dok *Ethereum* koristi Solidity, programski jezik razvijen za pisanje pametnih ugovora utemeljen na Java Scriptu. Hyperledger, projekt Linux Foundationa, koristi programski jezik go, razvijen u Googleu.[53] Općenito, tehnologija ulančanih blokova izrazito je fleksibilna te sustavi ulančanih blokova mogu biti napisani na raznim programskim jezicima, kao i aplikacije unutar virtualnih strojeva na ulančanim blokovima, koje mogu biti napisane svim podržanim programskim jezicima virtualnog stroja. Za hardversko programiranje infrastrukture ulančanih blokova, kao što su grafičke kartice i računalni procesori koriste se Open CL ili Cuda. Uloga hardvera i softvera u ulančanim blokovima opisana je u poglavlju „Tehnički aspekti i obilježja“.

Internet olakšava i ubrzava komunikaciju između geografski udaljenih ljudi, proizvod te komunikacije mnogi su hvalevrijedni projekti nastali isključivo u okruženju mreže. U užem

[53] Hyperledger, About Hyperledger (Linux Foundation, 2018.) URL: https://www.hyperledger.org/about

smislu ulančani blokovi mogu se interpretirati kao mrežna tehnologija. Rudarenje ulančanih blokova aktivnost je distribuiranog računarstva, dok je razvoj ulančanih blokova proizvod komunikacije i suradnje mnoštva ljudi na internetu. Razni projekti distribuiranog korištenja računala preteča su ulančanim blokovima, te su iskustva i interes za takve projekte indirektno omogućili razvoj ulančanih blokova. Na primjer, projekt distributed.net za cilj je imao demonstrirati *brute-force* napade na kriptografiju, te je zajednička moć računala spojenih na mrežu 1997. godine omogućila prvo probijanje 64-bitnog kriptografskog ključa.[54] Projekt SETI@home bio je najveći projekt distribuiranog računarstva sve do pojave ulančanih blokova. Naime, 1999. godine projekt je bilježio 5 milijuna učesnika koji su procesorsku snagu svojih računala posvetili analiziranju radio valova u svemiru s ciljem pronalaska života izvan Zemlje.[55, 56] Bitcoin, prva tehnologija ulančanih blokova svoj uspjeh duguje zajednici entuzijasta povezanih putem interneta. Ulančani blokovi razvijeni su na mreži, koriste komunikaciju između računala kako bi omogućili funkcionalnost sustava, što otvara mogućnost interpretacije ulančanih blokova kao mrežne tehnologije.

Postoji mnoštvo argumenata za interpretiranje ulančanih blokova kao ekonomske tehnologije. Ulančani blokovi prvi se puta javljaju kao tehnologija e-trgovine (eng. *e-commerce*), koja omogućava pojedincima razmjenu novca, dobara i usluga anonimno i bez centralne institucije. Mogućnost sigurnog zapisivanja transakcija i povjerenje u sustav stvorili su plodno tlo za razvoj tržišta trgovine valutama. Ulančani blokovi započeli su kao tehnologija neovisna o tradicionalnom financijskom sektoru, no sve veći interes ekonomista i drugih financijskih stručnjaka za tehnologiju uzrokovale su promjenu shvaćanja tehnologije. Danas se ulančani blokovi smatraju disruptivnom financijskom tehnologijom. Financijska tehnologija u stvari je portfelj digitalnih alata i primijenjenih tehnologija kojima financijske institucije kao što su banke, investicijski fondovi i revizijske tvrtke poboljšavaju postojeće i stvaraju nove financijske usluge. Ulančani blokovi kao financijska tehnologija imaju potencijal revolucionalizirati usluge računovodstva, digitalnih novčanika, sigurnog plaćanja i udruženog knjigovodstva.

Sigurnost i funkcionalnost ulančanih blokova utemeljena je na kriptografiji te se stoga ulančani blokovi mogu smatrati kriptografskom tehnologijom. Od sustava javnih i privatnih

[54] Distributed.net, History and Timeline, (1997.) URL: http://www.distributed.net/Main_Page
[55] SETI@home, About SETI@home, (Berkeley, 2019.) URL: http://setiathome.berkeley.edu/sah_about.php
[56] Phil Hochmuth, SETI@Home project ends; no E.T., but the technology continues, (NetworkWorld, 2005.) URL: https://www.networkworld.com/article/2316765/data-center/seti-home-project-ends--no-e-t---but-the-technology-continues.html

ključeva, do zapisivanja transakcija u blokove i konsenzusnih algoritama, svaki se element sustava ulančanih blokova temelji na kriptografiji. Trenutni sustavi koriste enkripciju SHA-256, kriptografsku funkciju za sažimanje koju je dizajnirala Agencija za nacionalnu sigurnost SAD-a.

Ulančani blokovi mogu se interpretirati kao tehnologija kibernetičke sigurnosti jer je cilj ove platforme zaštiti podatke od neovlaštenog pristupa i mijenjanja. Ministarstvo unutrašnje sigurnosti SAD-a definira kibernetičku sigurnost kao zaštitu kiberentičkog prostora i infrastrukture od fizičkih i kibernetičkih prijetnji u obliku tradicionalnih zločina.[57] Ulančani blokovi predstavljaju sigurnosno rješenje za zaštitu od određenih vrsta kibernetičkih napada. Internet uređaja (eng. *IoT*) futuristička je paradigma koja će omogućiti komunikaciju između strojeva koji su tradicionalno funkcionirali bez spajanja na mrežu. U paradigmu IoT ulaze autonomni automobili, dronovi, kućanski aparati, ali i medicinske naprave. Porast sofisticiranosti i cjenovne pristupačnosti raznih uređaja povezanih na mrežu označit će i povećanje kibernetičkog prostora, a sigurna i privatna komunikacija između strojeva spojenih na mrežu predstavlja sigurnosni izazov čije je potencijalno rješenje upravo tehnologija ulančanih blokova.

2.4. ULANČANI BLOKOVI U KONTEKSTU ARHIVISTIKE

Iz perspektive arhivistike, ulančani blokovi mogu se interpretirati kao tehnologija dugoročnog digitalnog čuvanja zapisa. Tradicionalni ulančani blokovi poput Bitcoina čuvaju zapise o novčanim transakcijama, no zbog kriptografske prirode, u lanac se može upisivati bilo kakav oblik digitalnog zapisa. Victoria L. Lemieux piše: „Mnoge sadašnje i predložene primjene tehnologije ulančanih blokova bave se problemima čuvanja zapisa, nude novi oblik generacijskog korištenja, čuvanja i korištenja zapisa. Na primjer, ulančani blokovi mijenjaju način na koji se ustanovljuje autentičnost zapisa, pouzdanje se s pouzdane institucije premješta na ustanovljavanje autentičnosti utemeljeno na sustavu.“[58] Arhivistica Cassie Findlay također prepoznaje potencijal tehnologije da promjeni arhivističku praksu: „Decentralizirani arhiv utemeljen na ulančanim blokovima kao mehanizmu pohrane mogao bi ponuditi neosporivi prostor za pristupanje zapisima. Dokumenti i drugi podaci mogu se provjeriti kroz ulančane blokove – čak i kada aplikacija koju smo koristili da ih tamo stavimo

[57] Department of Homeland Security, Cybersecurity (DHS, 2019.) URL: https://www.dhs.gov/topic/cybersecurity
[58] Victoria Lemieux, Blockchain Technology for Recordkeeping, (University of British Clumbia, 2018.), 4

više ne radi. To je decentralizirani dokaz kojeg ne može obrisati ili mijenjati nitko; ni konkurent, ni treća strana, ni država.“[59]

Mnogi arhivisti već su pisali na ovu temu, u Hrvatskoj se posebno ističu Bralić, Stančić i Kuleš, koji u članku naslovljenom „A Model for Long-term Preservation of Digital Signature Validity: TrustChain“ opisuju shemu dugoročnog arhiviranja digitalno potpisanih dokumenata na međuinstitucijskoj mreži.[60] Victoria Lemieux nudi teorijski okvir vrednovanja ulančanih blokova kao arhivske tehnologije, članak nosi naslov „Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework“, a njen je glavni argument da inovativni sustavi ulančanih blokova mogu ponuditi vjerodostojno čuvanje zapisa utemeljeno na tradicionalnoj arhivističkoj praksi.[61] Alan Pelz-Sharpe, Rob Begley i Jon Bushell zagovaraju skepsu u korištenju ulančanih blokova za čuvanje zapisa u članku „Records Management & Blockchain: Proceed, but with caution“, a članak u detalje raspisuje problematiku povjerenja u ulančane blokove, pogotovo u kontekstu javne uprave, bankarstva i javnog zdravstva.[62] Neupitno je da tehnologija ulančanih blokova za arhiviste predstavlja potencijalno rješenje za dugoročno, sigurno čuvanje digitalnih zapisa, no primjena tehnologije ulančanih blokova daleko je šira od tradicionalne arhivske prakse, što će pokazati iduće poglavlje rada.

2.5. PRIMJENA TEHNOLOGIJE ULANČANIH BLOKOVA

Da je primjena tehnologije ulančanih blokova praktički neograničena može se iščitati iz raznih izvora. Melanie Swan na tu temu piše:

> O ulančanim blokovima trebali bismo razmišljati kao o zasebnoj grupi stvari kao što je internet – iscrpna informacijska tehnologija s gradacijom tehničkih nivoa i aplikacija za sve vrste registracije, popisivanja i razmjenjivanja imovine, uključujući sva područja financija ekonomije i novca; čvrste imovine (fizičko vlasništvo, nekretnine, vozila) i neopipljive imovine (glasovi, ideje, reputacije, naumi, zdravstveni podaci, informacije itd.). No koncept

[59] Cassie Findlay, Decentralised and inviolate: the blockchain and its uses for digital archives (RKRoundTable, 2015.) URL: https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/

[60] Vladimir Bralić, Hrvoje Stančić, Magdalena Kuleš, A Model for Long-term Preservation of Digital Signature Validity: TrustChain (INFuture, 2017.)
URL: https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain

[61] Victoria Lemieux, Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework, (Future Technologies Conference paper, 2017.)

[62] Alan Pelz-Sharpe, Rob Begley i Jon Bushell, Records Management & Blockchain: Proceed, but with caution
URL: https://docs.wixstatic.com/ugd/74369c_83ae4fe781914ab2ab6872cc9986769a.pdf

> ulančanih blokova još je više od toga, to je nova organizacijska paradigma za istraživanje, vrednovanje i premještanje svih kvanta (diskretnih jedinica) bilo kakve informacije i potencijalno za koordinaciju svih ljudskih aktivnosti na još većem razmjeru no što je to do sada bilo moguće.[63]

Iako se tvrdnja o potencijalnoj koordinaciji svih ljudskih aktivnosti čini ambicioznom, ovo će poglavlje pokazati raznolikost primjena tehnologije ulančanih blokova. Od logistike i transporta hrane do zaštite autorskih prava - recentni projekti javljaju se u obliku alternativnih kriptovaluta ili u obliku tehnološke podrške poslovanju. Prvi dio poglavlja sagledat će projekte primjene ulančanih blokova izvan konteksta kriptovaluta, dok će drugi sagledati najinovativnije postojeće alternativne kriptovalute kao i njihovu primjenu.

Ulančani blokovi kao podrška poslovanju i javnoj upravi najrecentniji je pristup tehnologiji koji ju udaljava od izvorne namjene sigurnog trgovanja putem interneta. Naime, kao što je pokazano u poglavlju 2.2., tehnički aspekti ulančanih blokova omogućuju mnogo više od puke razmjene vrijednosti. Bilježenje podataka, kojima je lako pristupiti, bez mogućnosti njihove naknadne izmjene i bez potrebe za skupim hardverom otvara vrata novim smjelim interpretacijama tehnologije. Popisivanje svih potencijalnih primjena ove tehnologije tema je koja zahtjeva detaljnije istraživanje no što ovaj rad može ponuditi, pa stoga ovo poglavlje predstavlja samo kratki pregled primjena ulančanih blokova kao podrške u poslovanju na slijedećim primjerima: zemljišne knjige, logistika opskrbe hranom, financijska tehnologija, javno zdravstvo, zdravstveni podaci, digitalni identiteti i glasanje.

Ideja o čuvanju zemljišnih knjiga prvi se puta javlja u južnoameričkoj državi Honduras. Riječ je, naime, o državi u kojoj je nedostatak pravne države omogućio otimanje privatnih posjeda putem bespravnog upisivanja u zemljišne knjige. Kao potencijalno rješenje za ovaj problem javljaju se ulančani blokovi, jer prava na vlasništvo jednom upisana u njih nije moguće naknadno izmijeniti. Gertrude Chavez-Dreyfuss za Reuters o ovoj inicijativi izvještava: „Honduras, jedna od najsiromašnijih država Srednje Amerike, dogovorila je projekt s Teksaškom tvrtkom Factom u kojem će razviti nepromjenjivi i sigurni sustav za bilježenje vlasništva koristeći tehnologiju na kojoj funkcionira bitcoin.“ Chavez-Dreyfuss tehnologiju opisuje na slijedeći način: „Ulančani blokovi su glavna knjiga svih transakcija ove digitalne valute i smatra ih se ključnom tehnološkom inovacijom bitcoina. Tehnologija se

[63] Melanie Swan, Blockchain: Blueprint for a New Economy (O'Reily, 2015.), 13

razvija i udaljava od digitalnih valuta, prema primjenama kao što su baze podataka koje bilježe vlasništvo i sustava provjere podataka.“[64]

Sustav logističke potpore u lancu opskrbe hranom koristeći ulančane blokove razvija Linux Foundation na platformi za ulančane blokove Sawtooth. Studija slučaja provedena u sklopu projekta bavi se jednim od najmanje transparentnih segmenata industrije hrane, ribom i morskim proizvodima. Platforma Sawtooth omogućava praćenje prehrambenog proizvoda od trenutka ulova, kroz cijelu distribucijsku mrežu do konzumacije koristeći etikete sa senzorima spojenim na internet. Riječ je o spoju tehnologije interneta stvari i ulančanih blokova, koji omogućuje povezivanje sitnih uređaja putem interneta i bilježenja različitih informacija u ulančane blokove. Razvojni tim projekta ovako opisuje svoju viziju: „Kako bi povezao digitalni i fizički svijet, Hyperledger Sawtooth bilježi put koji riba prolazi od oceana do stola. Poput ribe u studiji slučaja, IoT senzori mogu se dodati bilo kakvoj robi koju transportiramo, s mogućnosti praćenja vlasništva, posjedovanja i telemetrijskih parametara poput lokacije, temperature, vlage, kretanja, udaraca i naginjanja. Kupac može pristupiti potpunom zapisu podataka i vjerovati da su informacije kojima pristupa točne i potpune.“ Ovakav pristup dakle nudi mogućnost praćenja ne samo hrane, već i sve robe krhke ili kvarljive prirode koja se prevozi i preprodaje.

U području financijskih tehnologija, ulančani blokovi nude rješenja za mnoge tradicionalne probleme trgovanja. Na primjeru tržišta obveznica jasno je vidljivo kako ulančani blokovi mogu olakšati i ubrzati poslovanje. Prema istraživanju Linux Foundationa, konvencionalni sustavi za čuvanje zapisa o trgovanju nailaze na sljedeće prepreke: „praksa čuvanja zapisa razlikuje se od institucije do institucije te je usklađivanje glavnih knjiga kompleksan, skup i vremenski zahtjevan posao. Povijest vlasništva nad obveznicama često je fragmentirana i nepotpuna, a centralizirano upravljanje podacima omogućuje monopolizaciju. Podaci se mogu naknadno mijenjati što omogućava financijsku prijevaru. Nadalje, centralizirani sustavi imaju jednu točku kvara.“ Kao decentralizirani sustav, Hyperledger Sawtooth, nudi potencijalno rješenje za navedene probleme. „Koristeći ulančane blokove u trgovini obveznicama moguće je stvoriti konzistentnost toka podataka između institucija, osigurati cjelovitost, dosljednost, preciznost i nepromjenjivost zapisa o povijesti vlasništva, osigurati osjetljive podatke koristeći jedinstvenu hardversku konfiguraciju i onemogućiti

[64] Gertrude Chavez-Dreyfuss, Honduras to build land title registry using bitcoin technology, (Reuters, 2015.) URL: https://www.reuters.com/article/usa-honduras-technology/honduras-to-build-land-title-registry-using-bitcoin-technology-idINKBN0O01V720150515

monopolizaciju te proizvesti transparentnost i povjerenje.“[65] Osim Linux Foundationa, računalni div IBM također nudi proizvode i podršku za financijsko tržište. Baš kao i švedska inovacijska tvrtka Enigio Time sa svojim rješenjem trace:original za upravljanje financijskim instrumentima koji se izdaju u samo jednom primjerku (npr. zadužnice i sl.) pa je njima potrebno upravljati kao digitalnim izvornicima i razlikovati jedan digitalni izvornik od svih drugih mogućih digitalnih kopija tog izvornika.[66]

U članku za Business Insider, Peter Huminski opisuje kako ulančani blokovi mogu poboljšati zdravstvene usluge: „Zdravstvene institucije pate od nemogućnosti sigurnog dijeljenja podataka na raznim platformama. Bolja kolaboracija u razmjeni podataka između institucija poboljšala bi vjerojatnost precizne dijagnoze, poboljšala bi efikasnost liječenja i omogućila bi zdravstvenim sustavima da ponude jeftinije zdravstvene usluge. Ulančani blokovi omogućili bi bolnicama, osiguranicima i drugim stranama u zdravstvu da dijele pristup mrežama bez kompromitiranja sigurnosti i integriteta podataka.“[67] Bernard Marr za časopis Forbes prepoznaje pet primjena ulančanih blokova u javnom zdravstvu: upravljanje medicinskim podacima, razvoj lijekova i integritet opskrbnog lanca, plaćanje zdravstvenih usluga, medicinska istraživanja i sigurnost podataka.[68]

Također je zanimljiva i primjena ulančanih blokova u glasanju. Kao tehnologija bilježenja nepromjenjivih zapisa, ulančani blokovi nude transparentan način bilježenja glasova. Kratki izvještaj Europskog parlamenta na temu „Što ako tehnologija ulančanih blokova revolucionalizira glasanje?“ otkriva potencijal tehnologije da promijeni i poboljša demokratske procese. Philip Boucher piše: „Protokol ulančanih blokova nudi način bilježenja i provjeravanja zapisa koji je transparentan i distribuiran između korisnika. Tradicionalno, glasove bilježi, njima upravlja, broji i provjerava centralni autoritet. Glasanje putem ulančanih blokova omogućilo bi glasačima da preuzmu te zadatke na sebe, te da sami imaju kopiju zapisa o glasanju. Taj zapis se ne bi mogao mijenjati jer bi drugi glasači mogli usporediti promijenjeni zapis sa svojim zapisom. Nelegitimni glasovi ne bi se mogli dodati jer bi svatko mogao provjeriti jesu li glasovi kompatibilni s postavljenim pravilima. Glasanje putem

[65] Hyperledger, Sawtooth, (Linux Foundation, 2019.) URL: https://sawtooth.hyperledger.org/examples/bond.html
[66] EnigioTime, trace:original (EnigioTime, 2019.) URL: https://www.enigio.com/traceoriginal
[67] Peter Huminski, The technology behind bitcoin could revolutionize these 8 industries in the next few years (Business Insider, 2017.), URL: https://www.businessinsider.com/8-applications-of-blockchain-2017-7
[68] Bernard Marr, This is why blockchains will transform healthcare, (Forbes, 2017.) URL: https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/2/#3ef7d684229d

ulančanih blokova prebacilo bi moć i povjerenje s centralnih aktera, kao što su izborna povjerenstva i podržalo razvoj tehnološki omogućenog društvenog konsenzusa.“[69]

Sve navedene primjene imaju potencijal olakšati, poboljšati ili ubrzati određene aspekte poslovanja i ljudskog života, no osim u razvoju ideja, koji se najčešće odvija na engleskom jeziku, postoji problem njihovog prihvaćanja i provedbe. Na primjeru provedbe poboljšanja sustava glasanja zorno se može prikazati važnost prevedene terminologije. Naime, jedan izrazito važan demokratski proces unutar jedne jezične zajednice ne može se promijeniti ako poboljšanja nisu detaljno opisana u jeziku zajednice, kako bi nacionalna zakonodavna tijela mogla donijeti informiranu i educiranu odluku. To je naime i glavni argument ovog rada kao i stav autora o jezičnom pristupu novim tehnologijama, te je tim argumentom opravdana potreba za prevođenjem i opisivanjem terminologije ove tehnologije na hrvatskom jeziku. Iduće poglavlje predstavit će osnove terminologije i terminografske prakse, znanja koja su potrebno kako bi se terminologija ulančanih blokova kvalitetno prevela i približila jezičnoj zajednici.

[69] European Parliamentary Research Service, What if blockchain technology revolutionised voting (European Parliament, 2016.)
URL:
http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA %282016 %29581918_EN.pdf

3. TERMINOLOGIJA I TERMINOGRAFIJA

Teresa M. Cabré terminologiju shvaća kao proces sakupljanja, opisivanja, obrađivanja i prezentiranja termina iz **specijaliziranih polja znanja** na jednom ili više jezika.[70] Specijalna polja znanja nužno stvaraju jezik struke, koji je skup termina nekog specijalnog polja znanja. Sager, Dungworth i McDonald ovako opisuju razliku između općeg jezika i jezika struke: „Priroda jezika je takva da opći jezik i jezik struke mogu postojati unutar jednog prirodnog jezika; osnovne karakteristike jezika manifestiraju se i u engleskom jeziku i u jeziku kemijskog inženjerstva, kako u francuskom tako i u jeziku fizike. Razlika između općeg jezika i jezika struke je razlika u količini, a ne vrsti, količini osnovnih karakteristika koje jezik maksimalno ili minimalno koristi. Jezik struke koristi se s više svijesti o jeziku od općeg jezika i situacije u kojima se koristi osnažuju korisnikovu brigu za jezik.“[71] Svrha svakog, pa tako i specijalnog jezika je komunikacija, a uspješna komunikacija na specijalnom jeziku unutar jezične zajednice zahtjeva upravljanje terminologijom i njezino prevođenje. Steurs, De Wachter i De Malsche o važnosti upravljanja terminologijom pišu: „prikladno upravljanje terminologijom ključno je za svakog stručnjaka koji radi sa specijaliziranim znanjem. Adekvatno upravljanje terminologijom povećava konzistentnost tekstova koji se proizvode, što ne samo da povećava njihovu iskoristivost i čitljivost, već i njihovu prevodivost na druge jezike.“[72]

Termin ili naziv, osnovna jedinica jezika struke nastaje u procesu zvanom primarna tvorba termina. Prijevod tako dobivenog termina i njegova prilagodba za korištenje na nekom drugom jeziku naziva se sekundarna tvorba termina. Sager detaljnije opisuje primarnu i sekundarnu tvorbu termina te tvrdi da u slučaju primarne tvorbe termina, termin nema lingvistički presedan. U slučaju sekundarne tvorbe, uvijek se koristi postojeći model. Primarna tvorba termina uglavnom je spontana, dok se sekundarnom može upravljati. Primarnom tvorbom naime nastaju novi termini, a sekundarnom se postojeći termini preuzimaju iz drugih jezika u obliku prevedenica, posuđenica i novotvorenica.[73] Sagerova podjela i njegovo shvaćanje tvorbe termina bilo je ključno u formiranju hrvatskih termina u

[70] M. Teresa Cabré, Terminology: Theory, Methods and Applications, (John Benjamins Publishing Company, 1999.), 25
[71] Juan C. Sager, David Dungworth, and Peter F. McDonald, English special languages: Principles and practice in science and technology, (Wiesbaden: Brandstetter, 1980.), 40
[72] Hendrik J. Kockaert, Frieda Steurs-Handbook of Terminology Volume 1 (John Benjamins Publishing Company, 2015), 18.
[73] Sager, Juan C. Term formation. Sue Ellen Wright and Gerhard Budin (eds.), Handbook of Terminology Management. Vol. 1: Basic Aspects of Terminology Management, (John Benjamins Publishing Company,1997.) 25−41.

terminološkoj bazi. O važnosti oblikovanja sekundarnih termina u kontekstu odnosa između jezika govori slijedeći izvadak iz Enciklopedije znanosti o prevođenju:

> U teoriji, praktični problem oblikovanja sekundarnih termina isti su svuda u svijetu, no u praksi postoje razlike između industrijski visoko razvijenih i slabije razvijenih jezičnih zajednica. Na primjer, jezične zajednice u Europi u najvećoj se mjeri sastoje od većinskih jezičnih zajednica, od kojih je svaka razvila standardni jezik koji uživa poštovanje i koriste ga formalno školovane zajednice. Jezik je potpuno razvijen za sve oblike i tehnike izražavanja te je stoga sposoban uvrstiti nove koncepte pristigle iz drugih jezičnih zajednica. Odnos prema oblikovanju sekundarnih termina u razvijenim je državama iz tog razloga nadgledan po principu *laissez-faire*, s ponekom intervencijom, zbog uvjerenosti da tradicija oblikovanja primarnih termina u nacionalnom jeziku može pronaći prihvatljiv spoj posuđivanja, prilagodbe, itd. Države bez takve tradicije smatraju razvoj jezika preduvjetom za, društveno blagostanje i ekonomski rast ili neizbježnom pojavomkoja ih prati. Razvoj jezika usko je povezan s tehnološkim napretkom, te se razvoj jezika smatra prvom fazom prijenosa tehnologije i industrijskog napretka.[74]

Imajući u vidu važnost oblikovanja sekundarnih termina u tehnološkom razvoju unutar jezične zajednice u sklopu ovog diplomskog rada izrađena je dvojezična terminološka baza tehnologije ulančanih blokova. Prema Cabré, kvalitetna terminologija na više jezika mora sadržavati slijedeće elemente: „uz ekvivalente na drugim jezicima, terminologija pripremljena za prevoditelje mora sadržavati kontekste koji nude informacije o korištenju termina i idealno nude informacije o konceptu kako bi omogućila prevoditeljima da koriste precizne oblike koji se odnose na specifični sadržaj.“[75] Iz tog razloga terminološka baza sastavljena u sklopu ovog diplomskog rada sadrži termine na engleskom i hrvatskom jeziku, njihovu definiciju na oba jezika te citate iz literature koji daju sadrže kontekst u kojem se koristi termin. Primjer jednog unosa u terminološku bazu pokazan je u Tablici 1. Ovo će poglavlje opisati temelje terminologije iz kojih proizlazi terminografska praksa, te predstaviti teoriju i savjete stručnjaka o sastavljanju terminološke baze kao i opisati osnovne pojmove i elemente terminološke baze.

[74] Mona Baker, Gabriela Saldanha Routledge Encyclopedia of Translation Studies 1st Edition (Routledge, 2001.), 249
[75] M. Teresa Cabré, Terminology: Theory, Methods and Applications, (John Benjamins Publishing Company, 1999.), 40

Tablica 1. - Primjer unosa u terminološku bazu

Term (EN)	**Definition**	**Citation**	**Syndetic relationship**
block	set of cryptographically recorded data with a header containing the hash of the previous block, a timestamp, a hash pointer and a nonce	A block is composed of multiple transactions and some other elements such as the previous block hash (hash pointer), timestamp and nonce. -Bashir, Mastering blockchain	NT: Genesis block RT: block header, timestamp, nonce
Termin (HR)	**Definicija**	**Citat**	**Sindetska veza**
blok	niz kriptografski zapisanih podataka sa zaglavljem koje sadrži hash vrijednost prijašnjeg bloka, vremensku oznaku, hash pokazivač i jednokratni niz	Blok se sastoji od više transakcija i neki drugih elemenata poput hash vrijednosti prijašnjeg bloka (hash pokazivača), vremenske oznake i jednokratnog niza. -Bashir, Mastering blockchain	Podređeni termin: inicijalni blok Povezani termini: zaglavlje bloka, vremenska oznaka, jednokratni niz

3.1. TERMINOGRAFSKA PRAKSA I TERMINOLOŠKA BAZA

Dva najvažnija djela o teoriji terminologije nastaju krajem 20. stoljeća, jedno u Francuskoj a drugo u Njemačkoj. Pierre Auger, 1988. godine napisao je knjigu naslovljenu „Méthodologie de la recherche terminologique“ (Metodologija terminološkog istraživanja) u kojoj prepoznaje tri pristupa u metodološkom radu: lingvistički, prevoditeljski i planski pristup.[76] Terminologija prilagođena lingvističkom pristupu bavi se konceptima i njihovom standardizacijom unutar jedne jezične zajednice te nudi strukturalni i funkcionalni opis specijalnog jezika. Terminologija prilagođena prevođenju prvi se puta javlja u višejezičnim društvima i organizacijama. Ovaj pristup najviše se fokusira ne na opisivanje terminologije, već na njeno ovladavanje stvaranjem terminoloških baza podataka, kako bi se premostile razlike između jezika i prevoditeljski problemi koji iz nje proizlaze. Treći pristup prilagođen je jezičnom planiranju, čiji je cilj strateškom intervencijom normalizirati korištenje nestabilnog jezika, koristeći pravne mjere i implementirane promjene. Cilj ovog pristupa je zamjena terminologije uvezene iz tehnološki dominantnih jezika, podupirući time stvaranje novih riječi unutar jezika.[77] Podjela o kojoj govori Auger odražava vrijeme u kojem je pisao,

[76] Pierre Auger, Méthodologie de la recherche terminologique, (Montreal: Office de la langue française, 1988.) 16

[77] M. Teresa Cabré, Terminology: Theory, Methods and Applications, (John Benjamins Publishing Company, 1999.), 224

danas bi se pristup metodologiji tehnologije vjerojatno dijelio na preskriptivni i deskriptivni ili na jednojezični, dvojezični i višejezični.

Drugo djelo od teorijskog značaja za terminologiju nosi naslov „Einführung in die allgemeine Terminologielehre und terminologische Lexikographie“ (Uvod u opću teoriju terminologije i terminološku leksikografiju) te ga je napisao Eugen Wüster 1991. godine. Wüster prepoznaje terminološku leksikografiju kao ključnu aktivnost terminologa te terminologiju smatra nerazdvojnom od leksikografske prakse.[78] Daria Protopescu za Sveučilišta u Budimpešti ovako opisuje Wüsterovu misiju i viziju: „Može se reći da je cijeli Wüsterov život bio posvećen terminologiji. Svojim radom htio je realizirati slijedeće ciljeve: a) eliminirati ambigvitet iz tehničkih jezika koristeći standardizaciju terminologije kako bi te jezike učinio djelotvornim alatima za komunikacija, b) uvjeriti sve korisnike tehničkih jezika u dobrobit standardizirane terminologije, c) utemeljiti terminologiju kao disciplinu za sve praktične svrhe i pridati joj status znanosti.“[79] Nadalje, važna je Wüsterova uloga u promicanju računarstva i informatike kao temelja kvalitetne terminografije. Naime, Wüster već u sedamdesetim godinama prošlog stoljeća prepoznaje potencijal računala: „Od svih do sad navedenih znanosti, računalna znanost je najnovija. To je znanost koja se bavi izgradnjom i korištenjem računala, koja se ne koriste samo u rješavanju matematičkih problema. Računala su također izvrsno tehničko pomagalo za jednu drugu znanost, koja je nešto starija od računalne: znanost o dokumentiranju i informacijama koja nosi naziv njemačkih korijena – informatika.“[80] Granica između računarstva, tj. računalne znanosti i informatike u međuvremenu je izbrisana, no činjenica je da se suvremena terminološka i terminografska praksa temelji na računalnim tehnologijama.

Osim što suvremena terminološka praksa koristi računala kako bi se ubrzali procesi zapisivanja, pretraživanja i pronalaženja termina, računala koriste terminologiju u mnogim procesima. Theresa M. Cabré piše: „Informatika također profitira zbog terminologije jer svi računalni programi povezani s bilo kojim aspektom jezika zahtijevaju terminologiju. [...] Procesi poput strojnog ili računalnog prevođenja, pretraživanje podataka, pomoći pri pisanju i komunikacije s bazama podataka. [...] Sustavi koji izvršavaju jezične aktivnosti (pisanje, korektura, prevođenje, itd.) koriste rječnike kao referentne točke za svaku operaciju

[78] Eugen Wüster, Einführung in die allgemeine Terminologielehre und terminologische Lexikographie (Romantischer Verlag, 1991), 67
[79] Daria Protopopescu, THEORIES OF TERMINOLOGY - PAST AND PRESENT, (University of Bucharest, 2006.), URL: cis01.central.ucv.ro/litere/activ_st/SCOL/revista.../PROTOPOPESCU.pdf
[80] Eugen Wüster, Die allgemeine Terminologielehre – Ein Grenzgebiet zwischen Sprachwissenschaft, Logik, Ontologie, Informatik und den Sachwissenschaften, (Linguistics, 197.), 61–106.

provjere.“[81] Stoga je posebno važno da je terminološka baza podataka čitljiva i razumljiva čovjeku, ali i lako prilagodljiva za korištenje u računalnim softverima čija je funkcija pisanje, korektura ili prevođenje. U novije vrijeme sve se više naglašava važnost kognitivnog pristupa terminologiji i jeziku struke. Pamela Faber, u knjizi „A Cognitive Linguistics View of Terminology and Specialized Language“ razjašnjava da se tradicionalni pristup terminologiji temelji na praktičnom opisivanju organizacije terminoloških baza, unosa termina i prepoznavanja termina u tekstu, dok je semantički aspekt terminologije zapostavljen. Rijetke su rasprave o metaforama u terminologiji, kognitivnom aspektu nastanku termina i ljudskih aktivnosti koje ih stvaraju. Glavni argument Pamele Faber jest da jezik struke nije samo registar ili način pisanja, već da se on sam može biti predmet istraživanja.[82] Usporedno nastaju i drugi suvremeni pristupi terminologiji, komunikacijska teorija terminologije, kako ju opisuje Cabré i sociokognitivna teorija terminologije kako ju opisuje Temmerman. U djelu naslovljenom „The Communicative Theory of Terminology, A Linguistic Approach of Terms“ Cabré opisuje sasvim nov pristup: Komunikacijska teorija terminologije lingvistički je pristup koji istražuje termine kao jedinice jezika, njihov kognitivni aspekt i društvenu funkciju.[83] Taj pristup ima daleko opsežniji pogled na terminologiju od tradicionalnog poimanja terminologije Eugena Wüstera, jer terminima pridaje metaforičku vrijednost. Rita Temmerman pak, u knjizi naslovljenoj „Toward New Ways of Terminology Description. The Sociocognitive Approach“ opisuje pristup utemeljen na konceptualnim sustavima, koji, unatoč svojoj apstraktnosti, omogućavaju više slobode u pisanju i interpretiranju termina od tradicionalne „Bečke škole“ terminologije. Temmerman zagovara onomasiološki pristup, koji termine podređuje konceptima u svijetu koji nas okružuje. Također, njen pristup zagovara eliminaciju slabo definiranih (eng. *fuzzy*) koncepata iz terminologije, jer terminološka struktura mora imati jasno definirane odnose podređenih i nadređenih pojmova. Temmerman tvrdi da se terminologija razvija konstantno, u sinkronicitetu s teorijom, te da analiza nastajanja termina nije primarna zadaća terminologije, već organizacija i intepretacija istih.[84, 85] Ideje Rite Temmerman na neki su način u srazu s preskriptivnim pristupima jezične politike

[81] M. Teresa Cabré, Terminology: Theory, Methods and Applications, (John Benjamins Publishing Company, 1999.), 55.
[82] Pamela Faber, A Cognitive Linguistics View of Terminology and Specialized Language (De Gruyter Mouton, 2000.)
[83] M. Teresa Cabré, The Communicative Theory of Terminology, A Linguistic Approach of Terms (Pub. Linguistiques, 2009.)
[84] Rita Temmerman, Toward New Ways of Terminology Description. The Sociocognitive Approach (John Benjamins Publishing Company, 2012.) 1-40
[85] Rosemarie Gläser, Review of Toward New Ways of Terminology Description. The Sociocognitive Approach, (Lexikos 14, 2004.), 434-439

opisanima u sljedećem paragrafu, no neupitno je da njen sociokognitivni pristup olakšava interpretaciju termina u kontekstu prevođenja i podučavanja terminologije.

Jezična politika u dva smjera igra važnu ulogu u stvaranju terminologije kao specijalnog jezika struke i razvoja struke unutar jezične zajednice. Terminološke smjernice UNESCO-a potvrđuju ovaj argument sljedećim riječima: „Ljudi čiji materinski jezik nije (ili nije dostatno) razvijen s gledišta terminologije i jezika struke (SPL) ili kojima je uskraćena uporaba njihova materinskog jezika u obrazovanju i usavršavanju, za pristup informacijama ili u međudjelovanjima na njihovim radnim mjestima, često su u nepovoljnome položaju.“[86] Nadalje, u Smjernicama upozoravaju da manjak razvoja terminologije i jezičnog planiranja može dovesti do niza negativnih posljedica: „Posljedica je toga da terminološko planiranje treba danas razumjeti u mnogo široj perspektivi inovacija i informacija, znanja, pa čak strategija e-sadržaja. Jezična zajednica čiji jezik nije razvio znanstvena i tehnička nazivlja prisiljen je upotrebljavati drugi, strani jezik za komunikaciju u određenom području.“[87] Upotreba drugog, stranog jezika u znanstvenom i tehničkom nazivlju, prema Smjernicama, vodi do slabije proizvodnje u istraživanju i razvoju, rjeđe upotrebe, težem zapisivanju i obradi tehnologije, slabijeg prijenosa znanja i na kraju manje primjene znanja unutar jezične zajednice.

Gradeći na temeljima teorije terminologije, ovaj rad preuzima mješavinu prevoditeljskog i planskog pristupa terminologiji, uzimajući u obzir važnost i kompatibilnost te iskoristivost terminologije u računalnim sučeljima. Rad terminologiju sagledava iz prevoditeljske perspektive kao sredstva koje pomaže premostiti jaz između tehnološki dominantnog jezika i tehnološki subordiniranog jezika. Inicijalno ovaj pristup javljao se kao formalni alat u višejezičnim društvima poput Francuskog Quebeca ili Belgije, no globalizacija i važnost računala u suvremenom životu učinile su svako društvo djelomično višejezičnim.[88] Daniel Dor u članku „Od Anglikanizacije do nametnute višejezičnosti: globalizacija, internet i politička ekonomija leksičkog koda“ razjašnjava ovu pojavu: „Proces globalizacije bez sumnje ima dalekosežne jezične posljedice, no tvrdim da one imaju manje veze sa širenjem engleskog jezika i smanjenjem jezične raznolikosti, već sa općom društvenom funkcijom jezika i odnosom između jezika, govornika, država i globalnog tržišta. Kako se ovi odnosi polagano mijenjaju, najbrže putem interneta, svjedočimo nastanku novih obrazaca korištenja,

[86] UNESCO, Smjernice za terminološke politike, (UNESCO, 2005.), 7.
[87] UNESCO, Smjernice za terminološke politike, (UNESCO, 2005.), 11.
[88] M. Teresa Cabré, Terminology: Theory, Methods and Applications, (John Benjamins Publishing Company, 1999.), 26.

standardizacije, održavanja i raznolikosti jezika – obrasci koji prije svega zadovoljavaju potrebe svjetskog potrošačkog tržišta.“[89] Spontani razvoj jezika, kako bi se prvobitno zadovoljile potrebe tržišta, često je nedostatan, te tehnologije koje ometaju tržišta zahtijevaju planski pristup kako bi jezik pratio najsuvremenije trendove.

Baza terminologije ulančanih blokova stoga će biti dvojezična, uzimajući u obzir važnost termina na tehnološki dominantnom, engleskom jeziku kao i njihovih ekvivalenata na hrvatskom. Prepoznajući međusobnu povezanost između terminologije i informatike, pogotovo u aspektima obrade prirodnog jezika, neobrađeni unosi u terminološku bazu nastalu tijekom pisanja ovog rada bit će slobodno dostupni na korištenje u obliku Excel tablice i online rječnika u obliku terminološke baze što će omogućiti efikasno izlučivanje i pretraživanje termina iz baze i njihovo korištenje u terminološkim bazama u sklopu alata za strojno potpomognuto prevođenje, izlučivanje definicija i njihovo korištenje u ekspertnim sustavima, izlučivanje veza između riječi za lingvističke softvere ili izlučivanje citata i konteksta iz baze za korištenje u višejezičnim korpusima. Takva prilagodba ima neke prednosti, ali i neke mane u odnosu na prikaz terminologije u obliku rječnika. Naime, prikaz sadržaja u rječniku u tiskanom obliku je pristupačniji čitatelju od nepregledne tablice, no iz takvog je prikaza teže automatski izlučiti informacije. Wüster s razlogom prepoznaje terminološku leksikografiju kao ključnu aktivnost popisivanja termina, no leksikografija je za razliku od terminologije ukorijenjena u tradicionalnim medijima kao što su rječnici i tezaurusi. Cabré s druge strane, nudeći nešto suvremeniji pristup, shvaća da je jedan od ključnih zadataka terminografije poboljšati računalno procesiranje prirodnog jezika.

Routledgeva Enciklopedija znanosti o prevođenju terminološku bazu definira kao svaki sustav koji čuva specijalizirani vokabular u elektroničkom obliku.[90] Uz istraživanje provedenom u sklopu diplomskog rada izrađena je terminološka baza, koja je u cijelosti priložena na kraju teksta, u Dodatcima diplomskom radu. Budući da se terminologija neprestano razvija, terminološka baza predstavlja sliku tehnologije u određenom trenutku. Termini su u svojim izvornim, engleskim oblicima prikupljeni iz recentne literature sredinom 2018. godine, a ponuđeni prijevodi ispitani su upitnikom provedenim početkom 2019.

[89] Danny Dor, From Englishization to Imposed Multilingualism: Globalization, the Internet, and the Political Economy of the Linguistic Code (Duke University Press, 2004.) 97-118
URL: https://muse.jhu.edu/article/54374/summary
[90] Mona Baker, Gabriela Saldanha, Routledge Encyclopedia of Translation Studies 1st Edition (Routledge, 2001.), 249

Provedeni upitnik i hipoteze koje su njime ispitane te rezultati upitnika detaljno su opisani u idućem, četvrtom poglavlju rada.

4. ISTRAŽIVANJE O TERMINOLOGIJI ULANČANIH BLOKOVA

4.1. ISTRAŽIVAČKA PITANJA I CILJ ISTRAŽIVANJA

Tijekom rada na izgradnji baze terminologije i rasprava s mentorima i drugim zainteresiranim pojedincima o tematici ulančanih blokova, učestalo su se javljala pitanja pristupa terminološkom opisivanju teme. Treba li termine prevoditi, ili ih ostavljati u originalnom obliku? Postoji li jezična potreba za terminološkom obradom ove teme? Kako prevesti pojedini termin? Opravdava li frekventnost korištenja nekog termina na hrvatskom jeziku njegovo uvrštavanje u terminološku tablicu? Teorija i praksa terminologije ne nude jednoznačan odgovor na ova pitanja, već nude niz deskriptivnih i preskriptivnih pristupa. Kako bismo ponudili odgovore na neka od postavljenih pitanja, u sklopu izrade baze terminologije provedeno je istraživanje čiji je cilj bio ispitati stavove i mišljenja relevantnih ispitanika o pristupu razvoju i popisivanju terminologije i samim terminima.

4.2. METODOLOGIJA

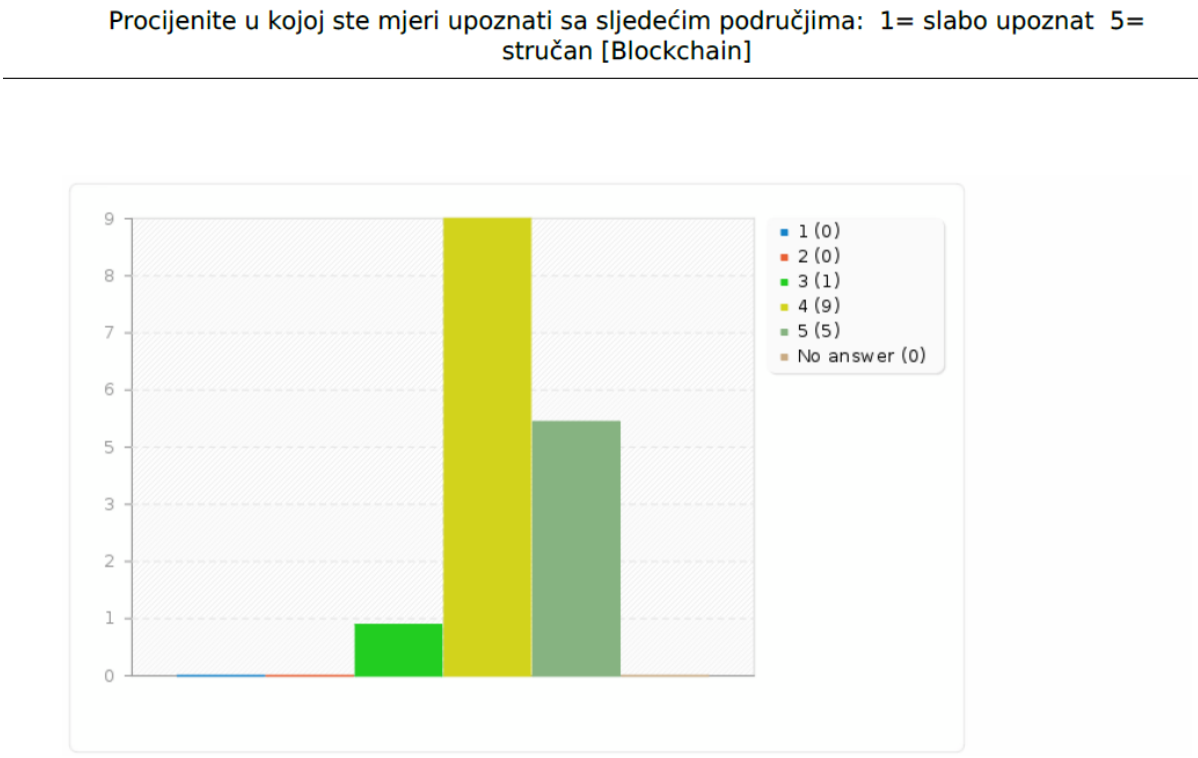
Istraživanje je provedeno u obliku online ankete poslane ispitanicima u ožujku 2019. Upitnik osmišljen u sklopu ovog istraživanja sastojao se od tri dijela. U prvome dijelu, naslovljenom *Osobni podaci*, prikupljeni su demografski podaci o dobi i spolu ispitanika te njihovim postignutim školskim obrazovanjem, poznavanjem engleskog jezika te procjenu vlastite upoznatosti sa sljedećim područjima: blockchain, DLT i kriptovalute. Drugi dio upitnika, naslovljen *Terminologija općenito* ispitivao je stavove ispitanika o pristupima razvoju terminologije ulančanih blokova. Treći dio nosi naslov *Termini* i ispitivao je konkretne primjere termina u kontekstu hrvatskog jezika, te su ispitanici zamoljeni da odaberu najbolja rješenja od ponuđenih ili da sami ponude rješenja za određene problematične termine.

Upitnik je poslan skupini stručnjaka, entuzijasta i istraživača koji se bave tehnologijom ulančanih blokova ili njenom primjenom u kriptovalutama. Od 49 ispitanika koji su pristupili upitniku, 34 unosa bilo je odbačeno zbog nepotpunih odgovora i nemogućnosti ispitivanja korelacijskih veza između odgovora. Ukupni broj ispitanika čiji su rezultati obrađeni bio je 15. Rezultati istraživanja prikazani su u sljedećem potpoglavlju.

4.3. REZULTATI

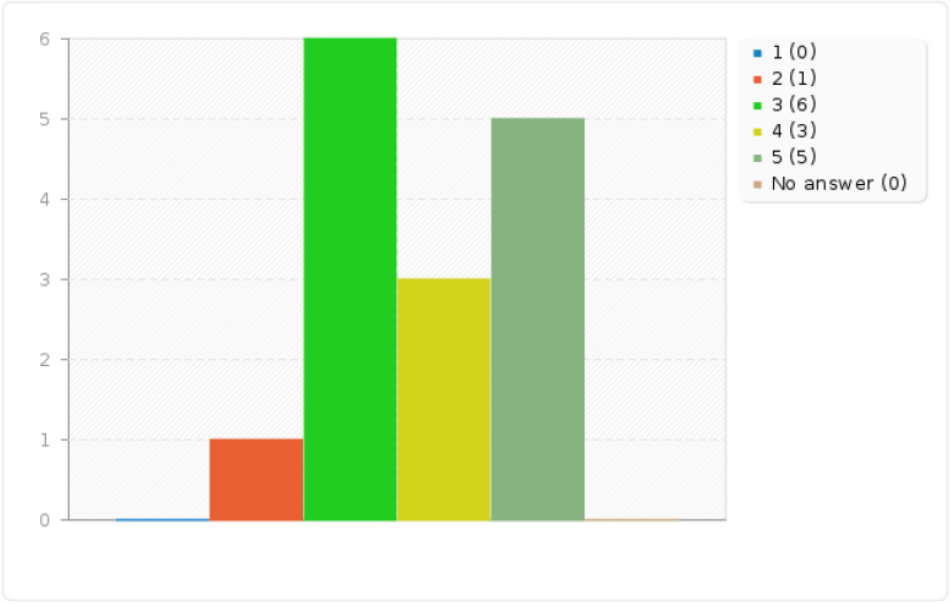
4.3.1. DEMOGRAFSKI PODACI

Uzorak ispitanika (N=15), starosne dobi između 24 i 46 godina, sastojao se od 2 osobe ženskog i 13 osoba muškog spola. Od 15 ispitanika, njih 4 postiglo je srednjoškolsko obrazovanje, 1 ispitanik završio je veleučilišni stručni studij, 1 preddiplomski, 7 diplomski studij i 2 poslijediplomski. 13 ispitanika procjenjuje svoje poznavanje engleskog jezika odličnim, između CEFR razina C1 i C2, dok preostala 2 ispitanika smatraju da je njihovo poznavanje jezika dobro, između razina B1 i B2. Na Likertovoj skali od 5 bodova ispitanici su procjenjivali svoju upoznatost s područjima Blockchain, DLT i kroptovalute. Ispitanici su svoju upoznatost ocjenjivali između najniže vrijednosti (1 = slabo upoznat) i najviše (5 = stručan). Srednja vrijednost odgovora za područje Blockchain iznosila je 4,27, što ukazuje na izvrsnu informiranost ispitanika u vezi ove teme. Ispitanici su nešto slabije bili upoznati s tehnologijom distribuirane glavne knjige, odnosno DLT. Srednja vrijednost upoznatosti s tim područjem iznosila je 3,8. Uzimajući u obzir mišljenja i opservacije iznesene u ovom radu, ne začuđuje da su ispitanici procijenili da najbolje poznaju područje kriptovaluta s rezultatom srednje vrijednosti 4,33. Rezultati upoznatosti ispitanika s određenim pojmovima prikazani su u Grafikonima 3, 4 i 5.

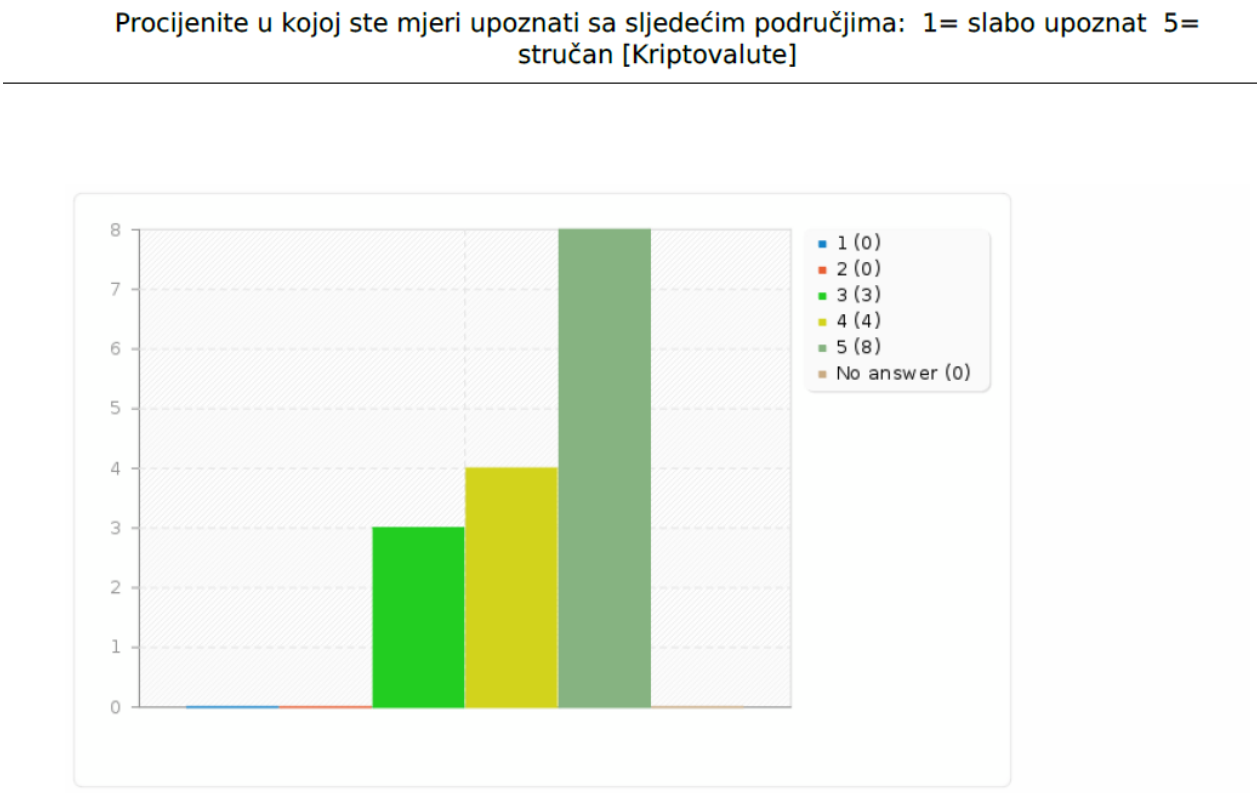


Grafikon 3. - Upoznatost s pojmom Blockchain

Procijenite u kojoj ste mjeri upoznati sa sljedećim područjima: 1= slabo upoznat 5= stručan [DLT]



Grafikon 4. - Upoznatost s pojmom DLT



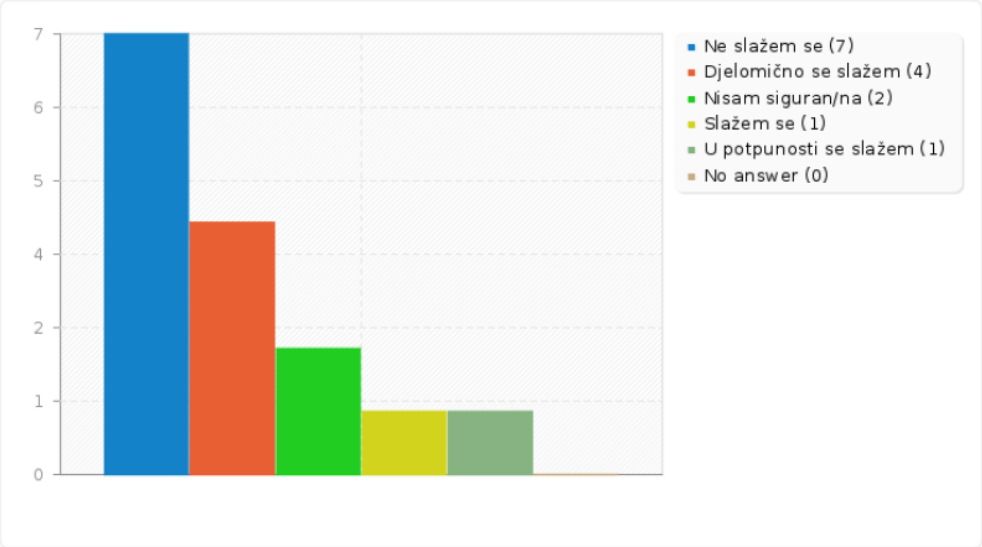
Grafikon 5. - Upoznatost s pojomo Kriptovalute

4.3.2. STAVOVI O TERMINOLOGIJI

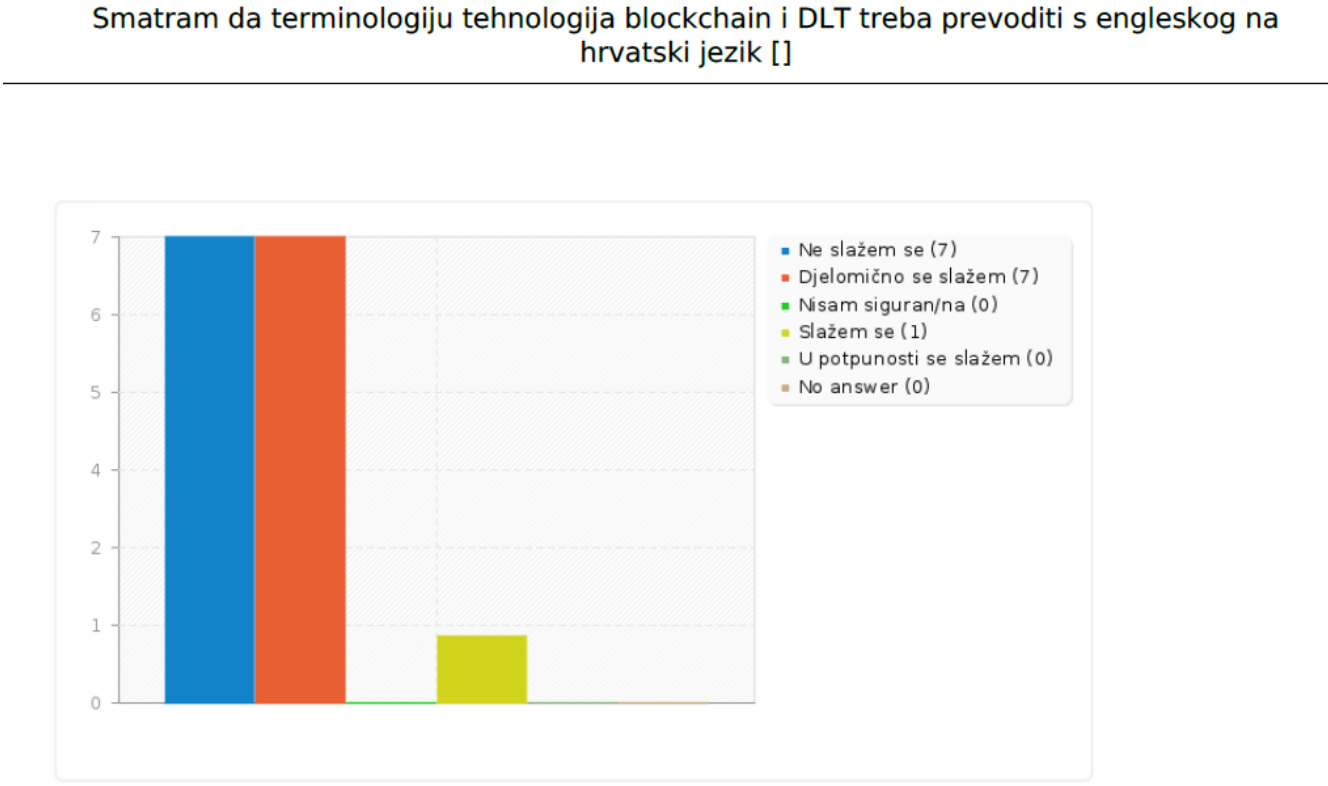
U dijelu upitnika naslovljenom *Terminologija općenito* ispitanici su odgovarali na pitanja o svojim stavovima u vezi prevođenja i popisivanja Blockchain terminologije. Na prva dva pitanja ispitanici su morali, na skali od jedan do pet bodova, izraziti svoje stavove o temi rada. Ponuđeni odgovori mjerili su slaganje ispitanika s određenom tvrdnjom koristeći sljedeće vrijednosti: (1) Ne slažem se, (2) Djelomično se slažem, (3) Nisam siguran/na, (4) Slažem se i (5) U potpunosti se slažem. Prva tvrdnja glasila je: *Prevođenje terminologije ulančanih blokova olakšat će stručnu komunikaciju u području ove tehnologije* te je većina ispitanika izrazila neslaganje s tvrdnjom (Grafikon 6.). Točnije, njih 7 ne slaže se s tvrdnjom, dok se 4 ispitanika samo djelomično slaže s tvrdnjom. Neutralno mišljenje o tvrdnji ima 2 ispitanika su odabrali Nisam siguran/na, a 1 ispitanik slaže se s tvrdnjom. Samo jedan ispitanik u potpunosti se slaže s tvrdnjom. Na drugu tvrdnju, *Smatram da terminologiju tehnologija blockchain i DLT treba prevoditi s engleskog na hrvatski jezik*, ispitanici su u velikoj većini dogovorili negativno (Grafikon 7.). Njih 7 ne slaže se s ovom tvrdnjom, dok se njih još 4 samo djelomično slaže s njom, a tek 1 ispitanik slaže se s tvrdnjom i još 1 ispitanik

u potpunosti se slaže. Rezultati ovog pitanja utjecali su na kasniju terminološku tablicu i pristup popisivanju terminologije, te je više anglizama uvršteno u stupac s hrvatskim terminima. Vizualni prikaz odgovora na ove dvije tvrdnje nalazi se na grafikonima 6 i 7.

Prevođenje terminologije ulančanih blokova olakšat će stručnu komunikaciju u području ove tehnologije. []



Grafikon 6. - Prevođenje terminologije olakšava stručnu komunikaciju



Grafikon 7. - Treba li prevoditi blockchain terminologiju

Drugi dio upitnika sadržavao je još jedno pitanje čiji je cilj bio procijeniti jezično okruženje u kojemu se kreću ispitanici. Konkretnije, pitanje daje uvid u stručnu komunikaciju povezanu s blockchain terminologijom te su ispitanici morali odabrati jednu od ove tri tvrdnje:

1. U profesionalnoj komunikaciji povezanoj s kriptovalutama ili tehnologijama blockchain i DLT najčešće koristim termine na engleskom jeziku
2. U profesionalnoj komunikaciji povezanoj s kriptovalutama ili tehnologijama blockchain i DLT najčešće koristim termine na hrvatskom jeziku
3. U profesionalnoj komunikaciji povezanoj s kriptovalutama ili tehnologijama blockchain i DLT najčešće koristim mješavinu termina na hrvatskom i engleskom

Većina ispitanika, njih 11 (73,33 %) odabrali su tvrdnju pod brojem 1, dok je njih 4, odnosno 26,67 %, odabralo tvrdnju pod brojem 3. Odgovori pokazuju da se ispitanici većinom koriste engleskim terminima u svojoj profesionalnoj komunikaciji, dok se neki koriste hrvatskim i engleskim terminima. Odgovori ukazuju da postoji potreba za obradom tematike na

hrvatskom jeziku jer je unutar jezične zajednice pristup znanju i informacijama povezanim uz ovu tehnologiju isključivo dostupan ljudima koji imaju izvrsno poznavanje engleskog jezika. U trenutku pisanja ne postoji niti jedan izvor u obliku rječnika ili glosara koji bi razjasnio i jezično približio ovu tematiku, a stručnjaci većinom koriste englesku terminologiju. Takav glosar ne bi nužno morao sve termine prevesti na hrvatski jezik, već ih može i kao posuđenice pokušati opisati na hrvatskom ako nemaju svoje uvriježene oblike u hrvatskom jeziku, na što ukazuju i odgovori posljednje skupine pitanja koja se bave samim terminima. Najvažnije je da se razvojem terminologije bave i stručnjaci u tom području i lingvisti koji su svjesni teorijske i praktične pozadine terminološkog rada.

4.3.3. ODABIR TERMINA

Cilj posljednje skupine pitanja, bio je ispitati korištenje odgovarajućih termina u hrvatskom kontekstu. Ovim dijelom upitnika ispitivali su se sljedeći termini: *blockchain, DLT, Cryptographic Hash Function, Mining, Timestamp, double spending, genesis block, P2P Network* i *PoW – Proof of Work algorithm*. Navedeni termini neki su od ključnih termina za opisivanje ulančanih blokova, a nemaju ustaljene terminološke ekvivalente na hrvatskom jeziku. Ispitanici su morali odabrati najbolji prijevod među ponuđenima ili sami ponuditi rješenje u obliku otvorenog odgovora. Svi termini bili su ponuđeni u sklopu rečenice na engleskom jeziku i njezinih različitih prijevoda na hrvatski jezik.

Prvo pitanje odnosilo se na termin Blockchain, te su ispitanici mogli birati između anglizma (posuđenice) i dvaju ponuđenih termina na hrvatskom (prevedenica). Grafikon 8. pokazuje pitanja i odgovore ispitanika.

Tablica 2. - Odgovori na pitanje vezano uz termin Blockchain

Koje je od ponuđenih rješenja najbolji ekvivalent ovoj rečenici na engleskom jeziku: "One solution is the Blockchain, a growing list of records which are linked and secured cryptographically."

ODGOVOR	BROJ	POSTOTAK
Jedno rješenje je blockchain, rastući niz zapisa koji su povezani i osigurani kriptografski. (A1)	10	66,67%
Jedno rješenje su ulančani blokovi, rastući niz zapisa koji su povezani i osigurani kriptograski. (A2)	4	26,67%
Jedno rješenje je lanac blokova, rastući niz zapisa koji su povezani i osigurani kriptografski. (A3)	1	6,67%

Kao što se vidi iz priložene slike, 10 ispitanika odlučilo se za posuđenicu blockchain, dok se njih 4 odlučilo za hrvatski oblik ulančani blokovi, a tek jedan ispitanik odabrao je kalk, odnosno doslovan prijevod lanac blokova. Rezultati ukazuju da većina ispitanika ne bi prevodila termin već ga ostavila u izvornom engleskom obliku, što je uzeto u obzir pri izradi terminološke tablice.

Sljedeći termin ispitan upitnikom bio je DLT, odnosno *Distributed Ledger Technology*. U ovom pitanju ispitanici su imali izbor između tri termina u hrvatskim rečenicama: *distributed ledger* tehnologija, tehnologija distribuirane glavne knjige i tehnologija zajednički vođene glavne knjige. Najpopularniji termin bio je *distributed ledger* tehnologija, njega je odabralo 46,67 % ispitanika, dok je drugi termin distribuirana glavna knjiga odabralo 33,33 % ispitanika. Najmanje ispitanika odlučilo se za termin zajednički vođena glavna knjiga, njih 20 %. Čini se da su ispitanici preferirali termin što bliži izvorniku, a ne onaj prilagođen hrvatskom jeziku. Unatoč tome, važno je napomenuti da engleska riječ *ledger,* inače računovodstveni termin, ima svoj ustaljeni i prihvaćeni oblik na hrvatskom, glavna knjiga. Uzimajući u obzir da je većina ispitanika odabrala anglizam u hrvatskoj rečenici, očito je važno da se sam termin previše ne udaljava od izvornog termina. Stoga je potrebno ponuditi rješenje koje zadovoljava pravila standardnog hrvatskog jezika, ali i ne ostavlja dvojbe u tumačenju termina. Prijedlog autora je da se zadrži hrvatski red riječi i hrvatska terminologija, s engleskom pokratom u zagradi: tehnologija distribuirane glavne knjige (DLT).

Sljedeće pitanje bilo je otvorenog tipa, te je ispitivalo termin c*rpytographic hash function*. Pitanje je postavljeno na sljedeći način: *Kriptografija je jedan od osnovnih elemenata svakog sustava ulančanih blokova. Osnovna matematička funkcija koja osigurava integritet sustava na engleskom se naziva cryptographic hash function, kako biste na hrvatskom izrazili taj termin?* Za ovo pitanje posebno je zanimljivo da termin iz polja kriptografije već postoji u hrvatskom jeziku, no ispitanici nisu upoznati s njim te niti jedan ispitanik nije ponudio rješenje kriptografska funkcija sažimanja.[91, 92] Čak 7 ispitanika ponudilo je rješenje kriptografska hash funkcija. Unatoč tomu što u terminologiji kriptografije postoji ustaljeni prijevod ovog termina, u terminološku tablicu bit će uvrštena dva termina: kriptografska funkcija sažimanja na prvom mjestu i kriptografska hash funkcija na drugom

[91] c.f. Hrvatska enciklopedija – kriptografija
URL http://www.enciklopedija.hr/natuknica.aspx?ID=33988
[92] c.f. Milan Pavlović, Implementacija i vizualizacija funkcije sažimanja SHA-3
URL: https://zir.nsk.hr/islandora/object/foi %3A1204

zbog učestalosti javljanja ovog termina, kako u spontanoj jezičnoj produkciji kod ispitanika, tako i u znanstvenim i drugim hrvatskim tekstovima na temu kriptografije na Internetu.

Četvrto pitanje u skupini odnosilo se na engleski termin *mining,* te je glasilo: *Kako biste na hrvatskom nazvali aktivnost u kojem računalo koristi procesorsku snagu kako bi gradilo sustav ulančanih blokova?* Ispitanici su na pitanje nudili odgovore otvorenog tipa, te su sami upisivali tekst. Većina rješenja sadržavala je ili anglizam *mining* (3), ili hrvatsku prevedenicu rudarenje (5). Zanimljivo je da termin *mining,* u digitalnom kontekstu, u hrvatskom već ima ustaljeni oblik zbog poslovne aktivnosti upravljanja podataka zvane *data mining,* odnosno rudarenje podataka. Unatoč tome što je riječ o sasvim različitim aktivnostima, termin rudarenje se u kontekstu ulančanih blokova javlja u spontanom izričaju ispitanika, što ukazuje na to da će termin biti bolje prihvaćen ako se njemu sličan termin već koristi u nekom drugom području. Nadalje, unatoč tome što su ispitanici većinom tvrdili da ne koriste hrvatske termine u komunikaciji povezanoj s ulančanim blokovima, odgovori na ovo pitanje pokazali su suprotno.

Sljedeći termin ispitan upitnikom bio je t*imestamp*, termin koji u hrvatskom ima svoj ustaljeni oblik od početka korištenja digitalnih potpisa u poslovnoj komunikaciji. Ponuđeni su bili odgovori vremenski žig, vremenska oznaka i vremenski pečat te su korisnici mogli dodati svoj odgovor. Njih 6, odnosno 40 % odabralo je najneutralniji pojam vremenska oznaka*,* dok je njih 4 (26,67 %) odabralo već prihvaćeni pojam vremenski pečat, dok se 20 % ispitanika odlučilo se za rješenje *Vremenski žig* unatoč tome što je ekvivalent engleskog pojma *stamp* pečat, a ne žig, čiji je engleski ekvivalent *seal.* Još 2 ispitanika, odnosno njih 13,33 % odabralo je upisati svoje rješenje, te su upisali anglizam *timestamp.*

U sljedećem pitanju ispitan je termin problematičan prilikom izrade terminološke tablice *double spending*. Rezultati upitnika nažalost nisu ponudili jednoznačan odgovor, kao što se vidi iz grafikona 9.

Tablica 3. - Rezultati petog pitanja na upitniku

Odaberite ekvivalent engleskog termina "double spending" na hrvatskom jeziku. Ukoliko ne biste iskoristili nijedan od navedenih termina, upišite termin koji koristite.

ODGOVOR	BROJ	POSTOTAK
Dvostruko trošenje (A1)	5	33,33%
Dvostruka transakcija (A2)	5	33,33%
Other	5	33,33%
No answer	0	0,00%

ID	SLOBODNI ODGOVOR
3	ostavio bi eng ili opcija 1.
18	double spending
19	Dupli trošak
29	dupla transakcija
46	kopirana transakcija

Iz rezultata se vidi da se jednaki broj ispitanika odlučio za rješenja dvostruko trošenje i dvostruka transakcija. Stoga će se u terminološku tablicu uvrstiti oba pojma, a vrijeme i jezična ekonomija pokazat će koji će od njih postati uvriježen prijevod za ovaj termin. Zbog deskriptivne prirode rada i uzimajući u obzir da oba termina funkcioniraju u kontekstu hrvatskog jezika, oba rješenja su prihvatljiva. S druge strane, moguća je i pojava termina duplo trošenje, koji je najpreciznij. Ovaj unos u terminološku tablicu stoga će imati tri termina na hrvatskom.

Sedmo pitanje odnosilo se na termin *genesis block* koji je posebno zanimljiv zbog biblijskih konotacija. Naime *genesis block* odnosi se na prvi zapis nekog sustava ulančanih blokova, iako bi najjednostavnije bilo nazvati ga prvim blokom, takvo ime ne bi bilo dostatno jer njegova važnost seže daleko iznad činjenice da je prvi. *Genesis block* temelj je sustava ulančanih blokova na kojemu se gradi cijeli lanac, a sadrži pravila i informacije o sustavu, ali i potencijalnu poruku autora (vidi str. 22). Prijedlog autora je da se kao ekvivalent *genesis block* prihvati inicijalni blok, s čime su se i ispitanici složili u velikoj većini. Njih čak 12, odnosno 80 %, odlučilo se za rješenje inicijalni blok.

ZAKLJUČAK

Blockchain, odnosno tehnologija ulančanih blokova, prema svim pokazateljima može se smatrati disruptivnom tehnologijom. Uzimajući u obzir definiciju potonjega pojma, disruptivne tehnologije imaju potencijal drastično promijeniti određeni aspekt ljudskog života. U kontekstu ulančanih blokova riječ je o čuvanju zapisa svih vrsta, poglavito imovine, bilo financijske ili fizičke, ali i neopipljivih zapisa poput glasova ili zdravstvenih podataka. Ulančani blokovi nude novi, revolucionarni pristup koristeći distribuirano povjerenje. Naime, povjerenje u sustav ne proizlazi iz treće strane već iz njegove matematičko-kriptografske sposobnosti da pohranjuje bilo koju vrstu digitalnog zapisa, bez mogućnosti izmjene i naknadne manipulacije.

Prepoznavanje potencijala ovakve digitalne revolucije upravo je bila i motivacija za pisanje ovog rada. Literatura iz područja terminologije naglašava važnost razvoja terminologije unutar jezične zajednice iz mnoštva razloga, od kojih je po mišljenju autora najvažniji razlog da razvoj terminologije omogućava jezičnoj skupini da ovlada, iskoristi, razvija i prenosi stručna znanja povezana s novim tehnologijama. Neupitno je da ovladavanje terminologijom nadolazećih tehnologija može dovesti do boljitka unutar jezične zajednice, jer društvo koje ovladava, iskorištava, razvija i prenosi znanja omogućava pojedincima unutar te jezične zajednice ili društva lakši pristup informacijama, bolje razumijevanje i brže učenje.

Stoga je u sklopu ovog diplomskog rada nastala terminološka baza u kojoj su na engleskom i hrvatskom jeziku razjašnjeni ključni pojmovi povezani s tehnologijom ulančanih blokova. U vezi s pojmovima provedeno je ispitivanje koje je uključivalo stručnjake i entuzijaste za ovu novonastalu suvremenu tehnologiju. Pokazalo se da je u procesu izrade terminologije povezane s novom tehnologijom osobito važno razjašnjavanje tih pojmova na hrvatskom jeziku. Time se omogućuje pristup znanju stručnog područja u nastajanju koje nije ograničeno poznavanjem jezika. Aktivnosti ovog diplomskog rada provedene su u nadi da će biti primjer dobre prakse u obradi terminologije budućim generacijama studenata jezika, ali i informacijskih i komunikacijskih znanosti, čiji znanstveni rad može potaknuti pozitivne promjene i obogatiti hrvatski jezik u kontekstu novih tehnologija.

LITERATURA

Auger, Pierre, Méthodologie de la recherche terminologique, (Montreal: Office de la langue française, 1988.) 16

Back, Adam, Hashcash, (1997.) URL: http://hashcash.org/docs/hashcash.txt

Baker, Mona, Saldanha, Gabriela, Routledge Encyclopedia of Translation Studies 1st Edition (Routledge, 2001.), 249

Bashir, Imran, Deeper insights into decentralization, cryptography, Bitcoin and popular Blockchain frameworks, (Packt, 2017)

Becker, Georg, Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis, (Ruhr-Universitat Bochum, 2008.), 12
URL:http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/becker_1.pdf

Bernard, Zoe, Everything you need to know about Bitcoin, (Business Insider, 2018.) URL: http://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12/#but-satoshi-nakamoto-didnt-work-entirely-alone-3

Bralić, Vladimir, Stančić, Hrvoje, Kuleš, Magdalena, A Model for Long-term Preservation of Digital Signature Validity: TrustChain (INFuture, 2017.)
URL: https://www.researchgate.net/publication/321171227_A_Model_for_Long-term_Preservation_of_Digital_Signature_Validity_TrustChain

Buterin, Vitalik, Ethereum White Paper, URL: https://github.com/ethereum/wiki/wiki/White-Paper

Buterin, Vitalik, Ethereum White Paper, URL: https://whitepaperdatabase.com/ethereum-eth-whitepaper/

Cabré, M. Teresa, Terminology: Theory, Methods and Applications, (John Benjamins Publishing Company, 1999.), 26.

Cabré, M. Teresa, The Communicative Theory of Terminology, A Linguistic Approach of Terms (Pub. Linguistiques, 2009.)

Champion de Crespigny, Angus, Blockchain: the hype, the opportuinty and what you should do, (EY, 2018.), 2. URL: http://www.ey.com/Publication/vwLUAssets/ey-blockchain-the-hypethe-opportunity-and-what-you-should-do/ %24FILE/ey-blockchain-the-hypethe-opportunity-and-what-you-should-do.pdf

Chaum, David, World's first electornic cash payment over computer networks, (David Chaum, 1992.) URL: https://chaum.com/projects/eCash

Chavez-Dreyfuss, Gertrude, Honduras to build land title registry using bitcoin technology, (Reuters, 2015.) URL: https://www.reuters.com/article/usa-honduras-technology/honduras-to-build-land-title-registry-using-bitcoin-technology-idINKBN0O01V720150515

CNet, CyberCash open Net to small change, (1996.), URL: https://www.cnet.com/news/cybercash-opens-net-to-small-change/

Dai, Wei, B-money, (1998.) URL: http://www.weidai.com/bmoney.txt

Deloitte Centre for the Edge, Australia, Bitcoin, Blockchain and distribueted ledgers, caught between promise and reality, (Deloitte, 2018.), 9. URL: https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf

Department of Homeland Security, Cybersecurity (DHS, 2019.) URL: https://www.dhs.gov/topic/cybersecurity

Distributed.net, History and Timeline, (1997.) URL: http://www.distributed.net/Main_Page

Dor, Danny, From Englishization to Imposed Multilingualism: Globalization, the Internet, and the Political Economy of the Linguistic Code (Duke University Press, 2004.) 97-118 URL: https://muse.jhu.edu/article/54374/summary

Economist, Blockchains: The great chain of being sure about things, (Economist, 2015.) URL: https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things

Elliot, Francis, Chancellor Allistair Darling on brink of second bailout for banks, (The Times, 2009.) URL: https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h

EnigioTime, trace:original (EnigioTime, 2019.) URL: https://www.enigio.com/traceoriginal

Espinoza, Javier, Is It Time to Invest in Bitcoin?, (The Wall Street Journal, 2014.) URL: https://www.wsj.com/articles/how-to-decipher-cryptocurrencies-1411333011

European Parliamentary Research Service, What if blockchain technology revolutionised voting (European Parliament, 2016.) URL: http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA %282016 %29581918_EN.pdf

Faber, Pamela, A Cognitive Linguistics View of Terminology and Specialized Language (De Gruyter Mouton, 2000.)

Findlay, Cassie, Decentralised and inviolate: the blockchain and its uses for digital archives (RKRoundTable, 2015.) URL: https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/

Gläser, Rosemarie, Review of Toward New Ways of Terminology Description. The Sociocognitive Approach, (Lexikos 14, 2004.), 434-439

Goldman Sachs, Blockchain – The New Technology of Trust, (Goldman Sachs, 2019) URL: http://www.goldmansachs.com/our-thinking/pages/blockchain/

Gupta, Vinay, A Brief History of Blockchain (Harvard Business Review, 2017.), URL: https://hbr.org/2017/02/a-brief-history-of-blockchain

Haber, Stuart, Stornetta, W. Scott, How to Time-Stamp a Digital Document,(Autoridad de Certificacion, 1991.), URL: https://crl.anf.es/pdf/Haber_Stornetta.pdf

Hochmuth, Phil, SETI@Home project ends; no E.T., but the technology continues, (NetworkWorld, 2005.) URL: https://www.networkworld.com/article/2316765/data-center/seti-home-project-ends--no-e-t---but-the-technology-continues.html

Huminski, Peter, The technology behind bitcoin could revolutionize these 8 industries in the next few years (Business Insider, 2017.), URL: https://www.businessinsider.com/8-applications-of-blockchain-2017-7

Hyperledger, About Hyperledger (Linux Foundation, 2018.) URL: https://www.hyperledger.org/about

Hyperledger, Sawtooth, (Linux Foundation, 2019.) URL: https://sawtooth.hyperledger.org/examples/bond.html

HZN, TO 307 Ulančani blokovi i tehnologija elektroničke distribuirane glavne knjige, (Hrvatski zavod za norme, 2019.) URL: https://www.hzn.hr/

IBM, IBM Blockchain platform (IBM, 2018.) URL: https://www.ibm.com/blockchain/platform/

International Standards Office, ISO/TC 307, Blockchain and electronic distributed ledger technologies, (ISO, 2019.) URL: https://www.iso.org/committee/6266604.html

Jakobson, Markus, Juels, Ari, Proofs of work and bread pudding protocols (extended abstract) (Bell Labs, RSA, 1999.) URL: http://www.hashcash.org/papers/bread-pudding.pdf

James, Anthony, Origin of White Papers (Klariti, 2017.), URL: http://klariti.com/white-papers/origin-of-white-papers/

Kockaert, Hendrik J., Steurs, Frieda -Handbook of Terminology Volume 1 (John Benjamins Publishing Company, 2015), 18.

Lemieux, Victoria, Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework, (Future Technologies Conference paper, 2017.)

Lemieux, Victoria, Blockchain Technology for Recordkeeping, (University of British Clumbia, 2018.), 4

Marr, Bernard, This is why blockchains will transform healthcare, (Forbes, 2017.) URL: https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/2/#3ef7d684229d

Mills, David et al., Distributed ledger technology in payments, clearing, and settlement (Federal Reserve, 2016), 12 URL: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf

Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, (2008.), 1. URL: https://bitcoin.org/bitcoin.pdf

Narayanan, Arvind, Bonneau, Joseph, Felten, Edward, Miller, Andrew, Goldfede, Steven, Bitcoin and Cryptocurrency Technologies (Princeton University Press, 2016.), 45

PCMag, First Virutal, (1998.) URL: https://www.pcmag.com/encyclopedia/term/43226/first-virtual

Pelz-Sharpe, Alan, Begley, Rob i Bushell, Jon, Records Management & Blockchain: Proceed, but with caution
URL: https://docs.wixstatic.com/ugd/74369c_83ae4fe781914ab2ab6872cc9986769a.pdf

Protopopescu, Daria, THEORIES OF TERMINOLOGY - PAST AND PRESENT, (University of Bucharest, 2006.), URL:
cis01.central.ucv.ro/litere/activ_st/SCOL/revista.../PROTOPOPESCU.pdf

PWC, Blockchain Overview (PWC, 2018.) URL:
https://mytaxpartner.pwc.com/media/1247992/blockchain-overview.pdf

Sager, Juan C., Dungworth David, and McDonald Peter F., English special languages: Principles and practice in science and technology, (Wiesbaden: Brandstetter, 1980.), 40

Sager, Juan C., Term formation. Sue Ellen Wright and Gerhard Budin (eds.), Handbook of Terminology Management. Vol. 1: Basic Aspects of Terminology Management, (John Benjamins Publishing Company,1997.) 25−41.

Samman George, Seibold, Sigrid, Consensus: Immutable agreement for the Internet of Value (KPMG, 2018.), 2. URL: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

SETI@home, About SETI@home, (Berkeley, 2019.) URL:
http://setiathome.berkeley.edu/sah_about.php

Swan, Melanie, Blockchain: Blueprint for a New Economy (O'Reily, 2015.), 13-17

Szabo, Nick, Bit Gold (Blog, 2008.) URL: https://unenumerated.blogspot.hr/2005/12/bit-gold.html

Tapscott, Alex, Tapscott, Don – Blockchain Revolution (Portfolio, 2016.), 45

Temmerman, Rita, Toward New Ways of Terminology Description. The Sociocognitive Approach (John Benjamins Publishing Company, 2012.) 1-40

UK Government Office for Science, Distributed Ledger Technology: beyond block chain, (UK Government report, 2017.) URL:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

UNESCO, Smjernice za terminološke politike, (UNESCO, 2005.), 11.

William, Jacob, Blockchain: The Simple Guide To Everythng You need to Know, (Amazon, 2016)

Wüster, Eugen, Die allgemeine Terminologielehre – Ein Grenzgebiet zwischen Sprachwissenschaft, Logik, Ontologie, Informatik und den Sachwissenschaften, (Linguistics, 197.), 61–106.

Wüster, Eugen, Einführung in die allgemeine Terminologielehre und terminologische Lexikographie (Romantischer Verlag, 1991), 67

POPIS GRAFIKONA I TABLICA

GRAFIKONI

TABLICE

PRILOG 1

TERMINOLOŠKA BAZA

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
address	character string used as an unique identifier denoting senders and recievers in a transaction	Adresses are unique identifiers that are used in a transaction on the blockchain to denote senders and recipients. An address is usually a public key or derived from a public key. - Bashir, Mastering blockchain These identities are called addresses , in Bitcoin jargon. You'll frequently hear the term address used in the context of Bitcoin and cryptocurrencies, and that's really just a hash of a public key. - Narayanan et al, Princeton Bitcoin book Their ownership of bitcoins was associated with digital addresses (long strings of numbers) that	RT: Public key	**adresa**	niz znakova koji služe kao jedinstveni identifikator u označavanju pošiljatelja i primatelja unutar neke transakcije	Adrese su jedinstveni identifikatori koji se koriste u transakcijama u sustavu ulančanih blokova kako bi označili pošiljatelje i primatelje. Adresa je najčešće javni ključ ili proizlazi iz javnog ključa. - Bashir, Mastering blockchain Takvi identifikatori se nazivaju adresama u žargonu bitcoina. Termin adresa često se spominje u kontekstu bitcoina i kriptovaluta, u stvari je to hash vrijednost javnog ključa. - Narayanan et. al, Princeton Bitcoin book Njihovo vlasništvo nad bitcoinima povezano je s

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
		had two components: a public key that served as an address, and a private key that gave its owner exclusive access to any coins associated with That address. -Tapscott and Tapscott, Blockchain revolution				digitalnom adresom (dugim nizom znamenki) koja ima dvije komponente: javni ključ koji služi kao adresa i privatni ključ koji vlasniku daje pristup njegovom novcu povezanom s tom adresom. -Tapscott and Tapscott, Blockchain revolution

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
altcoin	cryptocurrency alternative to bitcoin, usually with a specific purpose	The vast majority of alt coins are derived from bitcoin's source code, also known as "forks." Some are implemented "from scratch" based on the blockchain model but without using any of bitcoin's source code. Alt coins and alt chains (in the next section) are both separate implementations of blockchain technology and both forms use their own blockchain. The difference in the terms is to indicate that alt coins are primarily used as currency, whereas alt chains are used for other purposes, not primarily currency. - Antanopulous, Mastering Bitcoin	BT: cryptocurrency	**alternativna kriptovaluta**, ***altcoin***	kriptovaluta različita od bitcoina, često ima specifičnu svrhu	Većina alternativnih kriptovaluta nastale su iz izvornog koda bitcoina, još ih se naziva i račvama. Neki su implementirani iz potpuno novog koda koji se temelji na modelu ulančanih blokova ali ne koriste izvorni kod bitcoina. Alternativne kriptovalute i alternativni ulančani blokovi različite su implementacije tehnologije ulančanih blokova te obje koriste vlastiti sustav ulančanih blokova. Razlika između pojmova ukazuje na to da se alternativne kriptovalute koriste kao novac, dok se alternativni ulančanih blokovi koriste za neke druge, ne novčane, svrhe. Antanopulous, Mastering Bitcoin

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
asymmetrical cryptography, asymmetric cryptography	cryptographic system which uses a pair of keys, the public key to encrypt dana and the private key to decrypt it	Asymmetric crpytography refers to a type of cryptography whereby the key that is used to encrypt the data is different form the key that is used to decrypt the data. Also known as publick key cryptography, it uses public and private keys in order to encrypt and decrypt data, respectively. - Bashir, Mastering blockchain	Syn: public key cryptography RT: public key, private key	**asimetrična kriptografija**	kriptografski sustav koji koristi par ključeva, javni ključ da kriptira podatke i privatni ključ da ih dekriptira	Asimetrična kriptografija odnosi se na vrstu kriptografije u kojoj je ključ koji se koristi za kriptiranje podataka različit od ključa koji se koristi za dekriptiranje podataka. Također poznata i pod nazivom kriptografija javnog ključa, ona koristi javne i privatne ključeve kako bi kriptirala i dekriptirala podatke. - Bashir, Mastering blockchain

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
bitcoin, BTC	cryptocurrency in the form of digital decentralized money which uses the blockchain to record transactions	In a precise and technical definition, Bitcoin is digital cash that is transacted via the Internet in a decentralized trustless system using a public ledger called the blockchain. - Swan, Blockchain: Blueprint for a new economy Bitcoin can be defined in various ways; it's a protocol, a digital currency, and a platform. It is a combination of peer-to-peer network, protocols and software that facilitate the creation and usage of the digital currency named bitcoin. Note that Bitcoin with a capital B is used to refer to the Bitcoin protocol, whereas bitcoin with a lowercase b is used to refer to bitcoin, the currency. - Bashir, Mastering blockchain	BT: cryptocurrency	bitcoin	kriptovaluta u obliku digitalnog decentraliziranog novca koja koristi ulančane blokove kako bi zapisivala podatke o transakcijama	Precizna i tehnička definicija bitcoina glasi: digitalna gotovina koja se prenosi putem interneta koristeći decentralizirani sustav bez povjerenja i javnu glavnu knjigu koja se naziva ulančanim blokovima. - Swan, Blockchain: Bluepring for a new economy Bitcoin se može definirati na više načina; to je protokol, digitalna valuta i platforma. To je spoj *peer-to-peer* mreže, protokola i softvera koji omogućavaju stvaranje i korištenje digitalne valute po imenu bitcoin. Potrebno je primijetiti da je Bitcoin s velikim početnim slovom ime za protokol, a bitcoin s malim početnim slovom ime za kriptovalutu. -Bashir, Mastering blockchain

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
block	set of cryptographically recorded data with a header containing the hash of the previous block, a timestamp, a hash pointer and a nonce	A block is composed of multiple transactions and some other elements such as the previous block hash (hash pointer), timestamp and nonce. -Bashir, Mastering blockchain A block is a container data structure that aggregates transactions for inclusion in the public ledger, the blockchain. The block is made of a header, containing metadata, followed by a long list of transactions that make up the bulk of its size. The block header is 80 bytes, whereas the average transaction is at least 250 bytes and the average block contains more than 500 transactions. A complete block, with all transactions, is therefore 1,000 times larger than the block header. - Antanopulous, Mastering blockchain	NT: Genesis block RT: block header, timestamp, nonce	blok	niz kriptografski zapisanih podataka sa zaglavljem koje sadrži hash vrijednost prijašnjeg bloka, vremensku oznaku, hash pokazivač i jednokratni niz	Blok se sastoji od više transakcija i nekih drugih elemenata poput hash vrijednosti prijašnjeg bloka (hash pokazivača), vremenske oznake i jednokratnog niza. -Bashir, Mastering blockchain Blok sadrži podatkovne strukture koje grupiraju i sažimaju transakcije za upis u javnu glavnu knjigu, odnosno ulančane blokove. Blok sadrži zaglavlje, koje sadrži metapodatke, nakon kojih slijedi dugačak niz transakcija koje zauzimaju većinu prostora bloka. Zaglavlje bloka veličine je 80 bajta, dok je prosječna transakcija veličine 250 bajta, a prosječni blok sadrži 500 transakcija. Blok, sa svim transakcijama, je stoga 1000 puta veći od zaglavlja bloka. - Antanopulous, Mastering

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
						blockchain

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
block difficulty	measure of computation power required to generate proof-of-work	To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases. -Nakamoto, Bitcoin whitepaper A network-wide setting that controls how much computation is required to produce a proof of work. -Antanopulous, Mastering bitcoin	BT: Block	zahtjevnost bloka	mjera računalne snage potrebne da se proizvede dokaz o radu	Kako bi mrežu prilagodili rastućoj brzini hardvera i promjenjivom interesu za održavanje čvorišnih računala tijekom vremena, zahtjevnost dokaza o radu određuje se pomoću kliznog prosjeka čiji je cilj omogućiti stvaranje prosječne količine bloka po satu. Ako se blokovi proizvode prebrzo, zahtjevnost raste. -Nakamoto, Bitcoin whitepaper

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
block header	data located at the beginning of a block, contains information on the previous block, the nonce, a timestamp and the merkle tree root	The block header consists of three sets of block metadata. First, there is a reference to a previous block hash, which connects this block to the previous block in the blockchain. The second set of metadata, namely the difficulty, timestamp, and nonce, relate to the mining competition, as detailed in Chapter 8. The third piece of metadata is the merkle tree root, a data structure used to efficiently summarize all the transactions in the block. -Antanopulous, Mastering bitcoin	BT: Block	zaglavlje bloka	podaci na početku bloka, sadrži informacije o prijašnjem bloku, jednokratnom zapisu, vremensku oznaku i Merkleovo stablo	Zaglavlje bloka sastoji se od tri seta metapodataka. Prvi set sastoji se od reference na prijašnju hash vrijednost bloka koja povezuje trenutni i prijašnji blok u sustavu ulančanih blokova. Drugi set sastoji se od metapodataka, zahtjevnosti bloka, vremenske oznake i jednokratnog niza koji su povezani s rudarenjem, kao što je opisano u poglavlju 8. Treći set metapodataka je Merkleovo stablo, struktura podataka koja efikasno sažima sve transakcije unutar bloka. -Antanopulous, Mastering bitcoin
block height	position of a block within the blockchain	A second way to identify a block is by its position in the blockchain, called the block height. The first block ever created is at block height 0 (zero) -Antanopulous, Mastering bitcoin		visina bloka	pozicija bloka unutar ulančanih blokova	Drugi način na koji se može identificirati blok je njegova pozicija u ulančanim blokovima, naziva visinom bloka. Prvi blok ikad stvoren ima visinu 0 (nula). -Antanopulous, Mastering bitcoin

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
block reward	recompense rewarded to the miner for the calculation of a new block	By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. - Nakamoto, Bitcoin whitepaper An amount included in each new block as a reward by the network to the miner who found the Proof-Of-Work solution. It is currently 25BTC per block. - Antanopulous, Mastering bitcoin	BT: Block	nagrada bloka	kompenzacija koju prima rudar čije je računalo izračunalo novi blok	Prema konvenciji, prva transakcija u bloku je posebna transakcija koja stvara novčić čiji je vlasnik stvaratelj bloka. To je poticaj čvorišnim računalima da održavaju mrežu, i nudi način da se novčići inicijalno distribuiraju i puste u cirkulaciju budući da nema središnjeg autoriteta koji bi ih izdavao. Stalno dodavanje konstantne količine novih novčića može se usporediti s rudarenjem zlata u kojem rudari troše sredstva kako bi dodali zlato u cirkulaciju. U slučaju kriptovaluta, troši se procesorsko vrijeme računala i struja. - Nakamoto, Bitcoin whitepaper Svota pridodana svakom novom bloku kao nagrada mreže za rudara koji je ponudio izračun za dokaz o radu. Trenutno je riječ o 25 bitcoina po bloku. -

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
						Antanopulous, Mastering bitcoin

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
blockchain	database in the form of a distributed ledger which stores unmutable records organized in cryptographically secured blocks	blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. -Iasiti and Lakhani, Harvard Business Review, The truth about blockchain A blockchain is a type of distributed ledger that is shared across a business network. Business transactions are permanently recorded in sequential, append-only, tamper-evident blocks to the ledger. All the confirmed and validated transaction blocks are hash-linked from the genesis block to the most current block, hence the name blockchain. -IBM, Blockchain basics It is the blockchain that replaces		**ulančani blokovi,** *blockchain*	baza podataka u obliku distribuirane glavne knjige u kojoj se bilježe nepromjenjivi zapisi organizirani u kriptografski osigurane blokove	Ulančani blokovi su otvorena, distribuirana glavna knjiga koja bilježi transakcije između stranaka efikasno, provjerljivo i trajno.- Iasiti i Lakhani, Harvard Business Review, The truth about blockchain Ulančani blokovi su vrsta distribuirane glavne knjige koju dijeli cijela mreža. Poslovne transakcije dugoročno se bilježe u nanizanim blokovima na koje se mogu isključivo dodavati novi blokovi te u kojima je svaka promjena jasno vidljiva. Svi potvrđeni i provjereni transakcijski blokovi povezani su hash vrijednostima od početnog bloka do najrecentnijeg bloka, pa upravo zbog toga nose ime ulančani blokovi. -IBM, Blockchain basics

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
		this trusted third party. A database that contains the payment history of every bitcoin in circulation, the blockchain provides proof of who owns what at any given juncture. This distributed ledger is replicated on thousands of computers—bitcoin's "nodes"—around the world and is publicly available. -Economist, The great chain of being sure about things				Upravo ulančani blokovi zamjenjuju povjerenje u treću stranu. Baza podataka koja sadrži povijest plaćanja svakog bitcoina u cirkulaciji - ulančani blokovi nude dokaz o vlasništvu u bilo kojem trenutku. Distribuirana glavna knjiga replicirana je na tisućama računala, bitcoinovim "čvorovima", diljem svijeta i dostupna je javnosti. -Economist, The great chain of being sure about things

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
Byzantine General's Problem	mathematical problem dealing with consensus on a distributed network	Satoshi Nakamoto's invention is also a practical solution to a previously unsolved problem in distributed computing, known as the "Byzantine Generals' Problem." Briefly, the problem consists of trying to agree on a course of action by exchanging information over an unreliable and potentially compromised network. -Antanopulous, Mastering bitcoin In this classic problem, the Byzantine army is separated into divisions, each commanded by a general. The generals communicate by messenger in order to devise a joint plan of action. Some generals may be traitors and may intentionally try to subvert the process so that the loyal generals cannot arrive at a unified plan. The goal of this	RT: Distributed consensus	Problem bizantskih generala	matematički problem konsenzusa u distribuiranoj mreži	Izum Satoshija Nakamote također je praktično rješenje za do tada neriješeni problem u distribuiranom računarstvu, poznat pod imenom 'problem bizantskih generala'. Ukratko, problem se bavi dogovaranjem o zajedničkom djelovanju razmjenjujući informacije preko nepouzdane i potencijalno kompromitirane mreže. -Antanopulous, Mastering bitcoin U ovom klasičnom problemu, Bizantska vojska podijeljena je na divizije kojima zapovijedaju generali. Generali komuniciraju putem glasnika kako bi napravili zajednički plan djelovanja. Neki generali mogu biti izdajnici i mogu namjerno narušiti proces dogovora kako lojalni generali ne bi mogli dogovoriti zajednički plan. Cilj problema je

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
		problem is for all of the loyal generals to arrive at the same plan without the traitorous generals being able to cause them to adopt a bad plan. It has been proven that this is impossible to achieve if one- third or more of the generals are traitors. - Narayanan et al, Princeton Bitcoin book				koordinirati sve lojalne generale da dogovore zajednički plan, bez da izdajnički generali mogu natjerati lojalne generale da se dogovore za loš plan. Dokazano je nemoguće postići dogovor ako je više od jedne trećine izdajničkih generala. -Narayanan et al, Princeton Bitcoin book

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
collision resistant hash function	cryptographic function in which two inputs cannot produce the same output	The first property that we need from a cryptographic hash function is that it's collision-resistant. A collision occurs when two distinct inputs produce the same output. -Narayanan et al. Princeton bitcoin book	BT: hash function	hash funkcija otporna na koliziju	kriptografska funkcija u kojoj dva ulaza ne mogu proizvesti isti izlaz	Prvo svojstvo koje se zahtijeva od kriptografske hash funkcije je otpornost na koliziju. Kolizija nastaje kada dva različita ulaza nude isti izlaz. -Narayanan et al. Princeton bitcoin book
consenus mechanism, consensus protocol	set of rules governing agreement on the blockchain network	This is guaranteed by the mixture of mathematical subtlety and computational brute force built into its "consensus mechanism"—the process by which the nodes agree on how to update the blockchain in the light of bitcoin transfers from one person to another. -Economist, The great chain of being sure about things		konsenzusni mehanizam, konsenzusni protokol	skup pravila koje uređuju suglasnost u mreži ulančanih blokova	To je zagarantirano spojem matematičke suptilnosti i čiste računalne sile ugrađene u "konsenzusni mehanizam" - proces u kojem se čvorišna računala usuglašavaju o tome kako će ažurirati ulančane blokove u kontekstu prijenosa bitcoina s jedne osobe na drugu. - Economist, The great chain of being sure about things

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
crpytocurrency	digital money based on the blockchain	Bitcoin is the first and largest decentralized cryptocurrency. There are hundreds of other “altcoin” (alternative coin) cryptocurrencies, like Litecoin and Dogecoin, but Bitcoin comprises 90 percent of the market capitalization of all cryptocurrencies and is the de facto standard. -Swan, Blockchain - blueprint for a new economy		kriptovaluta	digitalni novac utemeljen na ulančanim blokovima	Bitcoin je prva i najveća decentralizirana kriptovaluta. Postoje stotine drugih alternativnih kriptovaluta, poput Litecoina i Dogecoina, no Bitcoin drži 90 posto kapitaliziranog tržišta svih kriptovaluta te je *de facto* standard. -Swan, Blockchain - blueprint for a new economy
cryptograhic hash function	mathematical computationl algorithm which encrypts an input into a hiding output	Cryptographic hashes, such as the SHA256 computational algorithm, ensure that any alteration to transaction input — even the most minuscule change — results in a different hash value being computed, which indicates potentially compromised transaction input. -IBM, Blockchain basics		kriptografska funkcija sažimanja	matematički, računalni algoritam koji enkriptira neki ulaz u zakriveni izlaz	Kriptografska hash funkcija, kao što je računalni algoritam SHA256, osigurava da bilo kakva promjena transakcijskog unosa, čak i najmanja promjena, uzrokuje promjenu hash vrijednosti, koja ukazuje na potencijalnu kompromitiranost ulazne vrijednosti. -IBM, Blockchain basics

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
cryptography	the practice of mathematically ensuring secure communication	Cryptographers use mathematics to define primitives, protocols, and their desired security properties in a formal way, and to prove them secure based on widely accepted assumptions about the computational hardness of specific mathematical tasks. - Narayanan et al, Princeton bitcoin book		kriptografija	praksa matematičke uspostave sigurne komunikacije	Kriptografi koriste matematiku kako bi definirali primitive, protokole i željena sigurnosna svojstva na formalan način i dokazali da su sigurni s pomoću široko prihvaćenih pretpostavki o težini izračuna specifičnih matematičkih zadataka. - Narayanan et al, Princeton bitcoin book

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
digital signature	an electronic string of symbols or code denoting identity	Specifically, cryptographic digital signatures enable a user to sign a digital asset or transaction proving the ownership of that asset. -Antanopulous, Mastering blockchain A digital signature is supposed to be the digital analog to a handwritten signature on paper. We desire two properties from digital signatures that correspond well to the handwritten signature analogy. Firstly, only you can make your signature, but anyone who sees it can verify that it's valid. Secondly, we want the signature to be tied to a particular document so that the signature cannot be used to indicate your agreement or endorsement of a different document. -Narayanan et al, Princeton bitcoin book		digitalni potpis	elektronički niz znakova ili kôd koji označava identitet	Konkretno, kriptografski digitalni potpisi omogućuju korisniku da potpiše digitalnu imovinu ili transakciju i dokaže vlasništvo nad njome. -Antanopulous, Mastering blockchain Digitalni potpis trebao bi biti istovjetan ručno napisanom potpisu na papiru. Dva svojstva su poželjna za uspostavu analogije između digitalnog i analognog potpisa. Kao prvo, samo potpisnik bi trebao moći na nešto staviti potpis, no bilo tko tko ga vidi mora moći potvrditi da je valjan. Kao drugo, digitalni potpis treba biti vezan uz određeni dokument kako ne bi bilo moguće isti potpis iskoristiti za suglasnost s nekim drugim dokumentom. -Narayanan et al, Princeton bitcoin book

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
		Digital signatures ensure that transactions originated from senders (signed with private keys) and not imposters. -IBM, Blockchain basics				Digitalni potpisi osiguravaju da su transakcije započele od pošiljatelja (potpisane privatnim ključem), a ne od prevaranta. -IBM, Blockchain basics

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
distributed consensus	agreement between all nodes in a peer-to-peer system	Consensus is the collaborative process that the members of a blockchain business network use to agree that a transaction is valid and to keep the ledger consistently synchronized. -IBM, Blockchain basics The implications of having a distributed consensus protocol reach far beyond this traditional application. If we had such a protocol, we could use it to build a massive, distributed key-value store, that maps arbitrary keys, or names, to arbitrary values. -Narayanan et al. Princeton bitcoin book		distribuirani konsenzus	suglasnost svih čvorova unutar *peer-to-peer* mreže	Konsenzus je proces suradnje kojeg članovi poslovne mreže ulančanih blokova koriste kako bi se složili da je transakcija važeća te kako bi glavnu knjigu održali konzistentno sinkroniziranom. -IBM, Blockchain basics Implikacije korištenja protokola distribuiranog konsenzusa sežu dalje od tradicionalnih primjena. Kada bismo imali takav protokol, mogli bismo ga iskoristiti da izgradimo golemo, distribuirano spremište ključnih vrijednosti, koje povezuje arbitrarne ključeve ili imena s arbitrarnim vrijednostima. -Narayanan et al. Pricneton bitcoin book

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
distributed ledger	a shared principal book	A distributed ledger is a type of database, or system of record, that is shared, replicated, and synchronized among the members of a network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network. This shared ledger eliminates the time and expense of reconciling disparate ledgers. -IBM, Blockchain basics		distribuirana glavna knjiga	dijeljena glavna knjiga	Distribuirana glavna knjiga oblik je baze podataka, ili sistema zapisivanja, koji je dijeljen, umnožen i sinkroniziran između članova mreže. Distribuirana glavna knjiga bilježi transakcije, kao što su razmjena imovine ili podataka, među korisnicima mreže. Ova dijeljena glavna knjiga eliminira vrijeme i trošak uspoređivanja dvije različite glavne knjige. -IBM, Blockchain basics
distributed ledger technology, DLT	family of technologies and application using a shared principal book	DLT refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants. -World Bank, DLT and blockchain fintech notes		tehnologija distribuirane glavne knjige, DLT	obitelj tehnologija i primjena koje koriste dijeljenu glavnu knjigu	DLT se odnosi na nov i brzo-evoluirajući pristup bilježenju i dijeljenju podataka kroz više spremišta podatka (ili glavnih knjiga). Ova tehnologija omogućava da se transakcije bilježe, dijele i sinkroniziraju kroz distribuirane mreže različitih učesnika. -World Bank, DLT and blockchain fintech notes

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
double spending, double spending attack	the act of using the same monetary unit or coin in two separate transactions	If the ledger is truly append-only, we can use it to defend against double-spending by requiring all transactions to be written the ledger before they are accepted. That way, it will be publicly visible if coins were previously sent to a different owner. - Narayanan et al, Princeton bitcoin book		dvostruka transakcija, dupla transkacija	korištenje iste obračunske jedinice ili istog novčića u dva plaćanja	Ako se u glavnu knjigu zaista mogu samo dodavati podaci, onda ju je moguće koristiti za zaštitu od dvostrukih transakcija postavljanjem zahtjeva da se sve transakcije upišu u glavnu knjigu prije no što budu prihvaćene. Na taj način javno je vidljivo ako ga je isti vlasnik ranije potrošio. - Narayanan et al, Princeton bitcoin book
fork	temporary state of a blockchain network in which two blocks occupy the same height on the chain	Forks occur as temporary inconsistencies between versions of the blockchain, which are resolved by eventual reconvergence as more blocks are added to one of the forks. - Antanopulous, Mastering bitcoin		račvanje	privremeno stanje mreže ulančanih blokova u kojem se dva bloka nalaze na istoj visini lanca	Račvanja se događaju kao privremene neusklađenosti između verzija ulančanih blokova, koje se rješavaju ponovnim usklađivanjem tako da se novi blokovi dodaju jednoj inačici.-Antanopulous, Mastering bitcoin
hash value	encrypted transaction data	Each transaction in a set that makes up a block is fed to a program that creates an encrypted code known as the hash value. -Economist, The		hash vrijednost	kriptirani podaci o transakcijama	Svaka transakcija u setu koji čini blok prolazi kroz program koji stvara kriptiranu vrijednost poznatu kao hash vrijednost. - Economist, The great chain of

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
		great chain of being sure about things				being sure about things
Merkle tree	hash value of all previous hashed values	Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. -Nakamoto, Bitcoin whitepaper		Merkleovo stablo	hash vrijednost svih prijašnjih hash vrijednosti	Kad se na zapis nove transakcije neke valute nadoveže dovoljno blokova, potrošenu transakciju može se obrisati kako bi se uštedjelo na diskovnom prostoru. Da bi se to izvelo bez kvarenja hash vrijednosti bloka, transakcije se sažimaju s pomoću Merkleovog stabla. Stari blokovi mogu se sažeti rezanjem grana na stablu. -Nakamoto, Bitcoin whitepaper

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
mining	using a computer's processor power to calculate new blocks	The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. -Nakamoto, Bitcoin Whitepaper Across the network, miners grind through trillions and trillions of possibilities looking for the answer. When a miner finally comes up with a solution other nodes quickly check it (that's the one-way street again: solving is hard but checking is easy), and each node that confirms the solution updates the blockchain accordingly. -Economist, The great chain of being sure about things		rudarenje	korištenje procesorske snage računala za izračunavanje novih blokova	Stalni rast količine novčića usporediv je s rudarima zlata koji troše svoje resurse kako bi dodali zlato u promet. U slučaju kriptovaluta, troši se vrijeme procesorskog rada i struja. -Nakamoto, Bitcoin Whitepaper U mreži rudari obrađuju trilijune i trilijune mogućih kombinacija tražeći odgovor. Kada rudar napokon dođe do izračuna, druga čvorišna računala brzo provode provjeru (to je vrlo jasna situacija, izračunavanje je zahtjevno, ali je provjera jednostavna), i svako čvorišno računalo koje potvrdi rješenje u skladu s time ažurira ulančani blok. -Economist, The great chain of being sure about things

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
mining pool	an association of blockchain miners	Once the purview of hobbyists, bitcoin mining is now dominated by large “pools”, in which small miners share their efforts and rewards, and the operators of big data centres, many based in areas of China, such as Inner Mongolia, where electricity is cheap. -Economist, The great chain of being sure about things		rudarsko udruženje	skup rudara ulančanih blokova	Nekad hobi, a danas rudarenjem bitcoina dominiraju velika rudarska udruženja u kojima rudari dijele trud i nagrade s operatorima velikih podatkovnih centara, kojih je mnogo u Kini, na primjer u središnjoj Mongoliji, gdje je struja jeftina. - Economist, The great chain of being sure about things
node	a computer connected to a blockchain network	every computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions -Swan, blockchain blueprint for a new economy		čvor	računalo spojeno na mrežu ulančanih blokova	Svako računalo povezano na bitcoin mrežu koje koristi klijentski softver koji izvodi zadatak potvrđivanja i prosljeđivanja transakcija. - Swan, blockchain blueprint for a new economy

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
nonce	a number string used to calculate a block	For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. -Nakamoto, bitcoin whitepaper The header then becomes part of a cryptographic puzzle solved by manipulating a number called a nonce. -Economist, The great chain of being sure about things		jednokratni niz	niz brojeva s pomoću kojih se izračunava blok	U mrežu za dodjeljivanje vremenskih oznaka uvodi se dokaz o radu ponavljanjem izračuna koristeći jednokratni niz u bloku dok se ne pronađe rješenje u kojem hash vrijednost bloka ima potreban broj bitova vrijednosti nula. -Nakamoto, bitcoin whitepaper Zaglavlje postaje dio kriptografske zagonetke koju se rješava manipuliranjem broja koji se naziva jednokratnim nizom. -Economist, The great chain of being sure about things

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
peer-to-peer	type of network utilizing computers on the same level, without hierarchy	A blockchain network for business is a collectively owned peer-to-peer network that is operated by a group of identifiable and verifiable participants. Participants may be individuals or institutions, such as a business, university, or hospital, for example. -IBM, Blockchain basics In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. -Nakamoto, Bitcoin Whitepaper		*peer-to-peer,* distribuirana mreža	vrsta mreže koja koristi ravnopravna računala, bez hierarhije	Mreža ulančanih blokova za poslovanje je mreža ravnopravnih računala u zajedničkom vlasništvu koju održava skupina korisnika čiji je identitet i provjerenost moguće ustvrditi. Korisnici mogu biti pojedinci ili institucije, kao što su na primjer privatna društva, sveučilišta ili bolnice. -IBM, Blockchain basics U ovom tekstu, predlažemo rješenje za dvostruke transakcije s pomoću distribuiranog servera koji izdaje vremenske žigove ravnopravnim računalima kako bi stvorio matematički dokaz o kronološkom redoslijedu transakcija. -Nakamoto, Bitcoin Whitepaper

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
permissioned blockchain	private blockchain network	Permissioned networks, on the other hand, are usually private and are limited to participants within a given business network. On permissioned blockchains, participants are allowed to view only the transactions relevant to them. Hyperledger is a collaborative effort, hosted by the Linux Foundation, to support the development of permissioned blockchains for business. -IBM, Blockchain basics	Syn: closed blockchain, private blockchain	zatvoreni sustav ulančanih blokova	privatna mreža ulančanih blokova	Zatvoreni sustavi ulančanih blokova, s druge strane, najčešće su privatni i sudjelovanje u njima je ograničeno na određenu poslovnu mrežu. U zatvorenim sustavima ulančanih blokova sudionici smiju pristupati samo transakcijama povezanima s njima. Hyperledger je suradnički projekt koji podržava Linux Foundation, čiji je cilj razvoj zatvorenih sustava ulančanih blokova namijenjenih poslovanju. -IBM, Blockchain basics
permissionless blockchain	public blockchain network	Permissionless networks are open to any participant, and transactions are verified against the pre-existing rules of the network. Any participant can view transactions on the ledger, even if participants are anonymous. Bitcoin is the most familiar example of a blockchain	Syn: open blockchain, public blockchain	otvoreni sustav ulančanih blokova	javna mreža ulančanih blokova	Otvoreni sustavi ulančanih blokova dostupni su bilo kome, a transakcije se potvrđuju po unaprijed određenim pravilima mreže. Bilo koji sudionik može pristupiti transakcijama u glavnoj knjizi unatoč anonimnosti sudionika. Bitcoin je najpoznatiji primjer mreže ulančanih blokova

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
		network that is permissionless and public. -IBM, Blockchain basics				koja je otvorena i javna. -IBM, Blockchain basics
private key	a string of numbers used to verify a digital signature	Digital signatures ensure that transactions originated from senders (signed with private keys) and not imposters. -IBM, Blockchain basics		privatni ključ	niz brojeva kojim se potvrđuje digitalni potpis	Digitalni potpisi osiguravaju da su transakcije započele od pošiljatelja (potpisane privatnim ključem), a ne od prevaranta. -IBM, Blockchain basics
proof of work	an algorythm which proves a computer's processor time was expended to calculate a nonce	For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. -Nakamoto, bitcoin whitepaper		*proof of work*, dokaz o radu	algoritam koji dokazuje da je procesorsko vrijeme računala iskorišteno kako bi se izračunao jednokratni niz	U mrežu za dodjeljivanje vremenskih oznaka, uveli smo dokaz o radu ponavljanjem izračuna koristeći jednokratni niz u bloku dok se ne pronađe rješenje u kojem hash vrijednost bloka ima potreban broj bitova vrijednosti nula. Jednom kad je procesorska snaga računala iskorištena kako bi zadovoljila dokaz o radu, blok se ne može

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
						mijenjati bez ponavljanja cijelog procesa. -Nakamoto, bitcoin whitepaper

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
smart contract	automated payment system on the blockchain	Smart contracts govern interactions with the ledger, and they can allow network participants to execute certain aspects of transactions automatically. For example, a smart contract could stipulate the cost of shipping an item that changes depending on when it arrives. With the terms agreed to by both parties and written to the ledger, the appropriate funds change hands automatically when the item is received. -IBM, Blockchain basics “Smart contracts” may be the most transformative blockchain application at the moment. These automate payments and the transfer of currency or other assets as negotiated conditions are met. For example, a smart contract might send a payment to		pametni ugovor	automatizirani sustav isplate na ulančanim blokovima	Pametni ugovori upravljaju interakcijama s glavnom knjigom, mogu dopustiti korisnicima mreže da izvrše neke vrste transakcija automatski. Na primjer, pametnim ugovorom može se urediti cijena poštarine nekog paketa koja se mijenja ovisno o tome kada bi paket trebao stići. Uvjeti s kojima se slože obje stranke zapisuju se u glavnu knjigu, te se prikladna uplata izvršava automatski po isporuci paketa. -IBM, Blockchain basics "Pametni ugovori" vjerojatno su najtransformativnija primjena ulančanih blokova danas. Oni automatiziraju uplate i transfer novca ili drugih vrijednosnica u trenutku kada su zadovoljeni dogovoreni uvjeti. Na primjer, pametni ugovor može poslati

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
		a supplier as soon as a shipment is delivered. --Iasiti and Lakhani, Harvard Business Review, The truth about blockchain				novac dobavljaču u trenutku kada pošiljka pristigne. - Iasiti i Lakhani, Harvard Business Review, The truth about blockchain

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
timestamp	data relating to time appended to a other dana	The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it. -Nakamoto, Bitcoin whitepaper		vremenska oznaka	podaci o vremenu dodani drugim podacima	Rješenje koje se predlaže počinje s poslužiteljem za vremenske oznake. Poslužitelj uzima hash vrijednosti bloka, pridružuje im vremensku oznaku te objavljuje hash vrijednost javnosti, putem novina ili na Usenetu. Vremenska oznaka dokazuje da su podaci postojali u to vrijeme, jer je dio hash vrijednosti. Svaka vremenska oznaka sadržava prijašnju vremensku oznaku u svojoj hash vrijednosti, stvarajući lanac u kojem svaka dodatna vremenska oznaka potvrđuje prijašnje. -Nakamoto, Bitcoin whitepaper
transaction	transfer of assets	A transaction is an asset transfer onto or off of the ledger. -IBM, blockchain basics		transakcija	transfer vrijednosti	Transakcija je transfer vrijednosti s nekog računa zabilježenog u glavnu knjigu ili na njega. - IBM, blockchain basics

Term (EN)	Definition	Citation	Syndetic relationship	Termin (HR)	Definicija	Citat
wallet	software which holds a user's cryptocurrencies	If you're storing your bitcoins locally, you'd typically use wallet software, which is software that keeps track of all your coins, manages all the details of your keys, and makes things convenient with a nice user interface. - Narayanan et al, Princeton bitcoin book		novčanik	softver koji čuva korisnikove kriptovalute	Ako se bitcoin čuva lokalno, tipično će se koristiti softverski novčanik. To je softver koji prati sav digitalni novac u posjedu korisnika, čuva detalje njegovim kriptografskim ključevima i olakšava korištenje nudeći jednostavno korisničko sučelje. - Narayanan et al, Princeton bitcoin book